COMBINATORIAL DESIGN THEORY - NOTES

Alexander Rosa

Department of Mathematics and Statistics,
McMaster University, Hamilton, Ontario, Canada

Combinatorial design theory traces its origins to statistical theory of experimental design but also to recreational mathematics of the 19th century and to geometry. In the past forty years combinatorial design theory has developed into a vibrant branch of combinatorics with its own aims, methods and problems. It has found substantial applications in other branches of combinatorics, in graph theory, coding theory, theoetical computer science, statistics, and algebra, among others. The main problems in design theory are, generally speaking, those of the existence, enumeration and classification, structural properties, and applications.

It is not the objective of these notes to give a comprehensive abbreviated overview of combinatorial design theory but rather to provide an introduction to developing a solid basic knowledge of problems and methods of combinatorial design theory, with an indication of its flavour and breadth, up to a level that will enable one to approach open research problems. Towards this objective, most of the needed definitions are provided.

I. BASICS

1. BALANCED INCOMPLETE BLOCK DESIGNS

One of the key notions in design theory, the notion of pairwise balance (or, more generally, t-wise balance), has its origin in the theory of statistical designs of experiments. Coupled with the requirement of a certain type of regularity, it leads to the notion of one of the most common types of combinatorial designs.

1991 *Mathematics Subject Classification.* .

A *balanced incomplete block design* (BIBD) with parameters (v, b, r, k, λ) is an ordered pair $(V, \mathcal{B})$ where V is a finite v-element set of *elements* or *points*, $\mathcal{B}$ is a family of k-element subsets of V, called *blocks* such that every point is contained in exactly r blocks, and every 2-subset of V is contained in exactly λ blocks.

In terms of graphs, a BIBD is an edge-disjoint decomposition of the complete multigraph λK_v into k-cliques.

The five parameters v, b, r, k, λ are not independent: simple counting yields two relations (1) $vr = bk$, and (2) $\lambda(v-1) = r(k-1)$. BIBDs are usually written as BIBD(v, k, λ) or (v, k, λ)-BIBD as the remaining two parameters can be deduced from (1),(2). Since both, $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{\lambda v(v-1)}{k(k-1)}$ must be integers, the necessary conditions for the existence of a BIBD(v, k, λ) are often written as
$\lambda(v-1) \equiv 0 \ (mod\ k-1)$, $\lambda v(v-1) \equiv 0 \ (mod\ k(k-1))$.

If $(V, \mathcal{B})$ is a (v, k, λ)-BIBD where $V = \{x_i : 1 \leq i \leq v\}$ and $\mathcal{B} = \{B_j : 1 \leq j \leq b\}$ then the *incidence matrix* of the BIBD is the $v \times b$ matrix $A = (a_{ij})$ where $a_{ij} = 1$ if $x_i \in B_j$ and =0 otherwise. The incidence matrix satisfies $AA^T = (r - \lambda)I + \lambda J$ where T indicates the transpose, I is the $v \times v$ identity matrix, and J is the $v \times v$ matrix of 1's. In the matrix $X = AA^T$, each diagonal element equals r, and each off-diagonal element equals λ.

A BIBD is *symmetric* if $v = b$ (and $r = k$).

Example 1. A $(7, 3, 1)$-BIBD (the "Fano plane", i.e. the projective plane of order 2).

123 145 167 246 257 347 356.

Example 2. A $(9, 12, 4, 3, 1)$-BIBD (the affine plane of order 3).

123 456 789 147 158 169 248 259 267 349 357 368 .

Example 3. A $(15, 7, 3)$-BIBD: elements are $V = \{0, 1, \ldots, 14\}$, blocks are

$B_0 :$ 0 1 2 3 4 5 6
$B_1 :$ 0 1 2 7 8 9 10
$B_2 :$ 0 1 2 11 12 13 14
$B_3 :$ 0 3 4 7 8 11 12
$B_4 :$ 0 3 4 9 10 13 14
$B_5 :$ 0 5 6 7 8 13 14
$B_6 :$ 0 5 6 9 10 11 12
$B_7 :$ 1 3 5 7 9 11 13
$B_8 :$ 1 3 7 10 12 14
$B_9 :$ 1 4 5 8 10 11 14
$B_{10} :$ 1 4 6 8 9 12 14
$B_{11} :$ 2 3 5 8 10 12 13
$B_{12} :$ 2 3 6 8 9 11 14
$B_{13} :$ 2 4 5 7 9 12 14
$B_{14} :$ 2 4 6 7 10 11 13

The BIBDs from Examples 1 and 3 are symmetric, the one from Example 2 is not. In a symmetric design, any two blocks have exactly λ elements in common.

Given a symmetric (v, k, λ)-BIBD with blocks $\mathcal{B} = \{B_i\}$, fix one of its blocks, say B_0, and obtain the blocks ${B_i}^*$ of its *derived* design by taking ${B_i}^* = B_0 \cap B_i$. The parameters of the derived design in terms of the original BIBD are

$v^* = k,\ b^* = b - 1,\ r^* = r - 1,\ k^* = \lambda,\ \lambda^* = \lambda - 1.$

The symmetric design from Example 3 yields a derived design which is a BIBD$(7, 14, 6, 3, 2)$.

Fixing again a block B_0 in a symmetric BIBD, deleting this block and its elements from all other blocks of the BIBD gives the *residual* design whose parameters are $v^" = v - k$, $v^" = v - 1,\ r^" = r,\ k^" = k - \lambda,\ \lambda^" = \lambda$.

The residual design of the symmetric design in Example 3 has parameters $v^" = 8,\ b^" = 14,\ r^" = 7,\ k^" = 4,\ \lambda^" = 3$.

A further necessary condition for the existence of a BIBD(v, b, r, k, λ) is given by *Fisher's inequality*: $b \geq v$. One way to prove this is to evaluate the determinant of X: $detX = (r - \lambda)^{v-1}(v\lambda - \lambda + r)$. To see this, subtract the first column from all others and then add rows $2, 3, \ldots, v$ to the first row; then all elements above the main diagonal equal 0; on the main diagonal, the first entry is $r + (v - 1)\lambda$, the rest are $r - \lambda$. We must have $r > \lambda$ since $r = \lambda$ would mean that each element is paired with each other whenever it is contained in a block, thus each block would contain all v elements. Thus X is nonisngular, A is of rank at most b, X is of rank v but the rank of the product cannot exceed the rank of its factors, therefore $b \geq v$ (it follows thar $r \geq k$).

Thus, for example, there cannot exist a $(21, 6, 1)$-BIBD, since $b = 14 < 21 = v$ even though the arithmetic necessary conditions (1), (2) are satisfied.

Another necessary condition for the existence of symmetric designs is given by the following.

In a symmetric BIBD, if v is even then $k - \lambda$ is a square.

Indeed, in a symmetric design $b = v$, so A is a square matrix, and $(det\ A)^2 = det\ X = (k - \lambda)^{v-1}(v\lambda - \lambda + k)$. Since $k(k - 1) = \lambda(v - 1)$, we have $v\lambda - \lambda + k = k(k - 1) + k = k^2$. But then the other factor of $det\ X$, namely $(k - \lambda)^{v-1}$ must also be a square and since v is even, this means that $k - \lambda$ must be a square as well.

Thus, for example, there cannot exist a symmetric $(22, 7, 2)$-BIBD (since $k - \lambda = 5$ is not a square) although necessary conditions (1), (2) are satisfied.

But the necessary conditions above taken together are still not sufficient for the existence of BIBDs. The parameter sets $(v, b, r, k, \lambda) = (22, 33, 12, 8, 4)$ or $(46, 69, 9, 6, 1)$ or $(111, 111, 11, 11, 1)$ all satisfy the arithmetic necessary conditions and are not covered by the additional necessary conditions given above. Nevertheless, in each of these cases it has been proved by means of a detailed structural analysis combined with a considerable computational power that the corresponding BIBD does not exist. The quest to obtain (necessary and sufficient) conditions for the existence of BIBDs is continuing. Currently, the "smallest" parameter sets for which the existence of a BIBD is undecided are $(51, 85, 10, 6, 1)$, $(61, 122, 12, 6, 1)$, $(40, 52, 13, 10, 3)$ and $(85, 170, 14, 7, 1)$. There exist extensive tables of parameters of "small" BIBDs (for example, with up to $r \leq 41$) that record for each parameter set whether the design exists, does not exist or its existence is an open question (together with some additional information including enumeration results).

A BIBD is *resolvable* if its blocks can be partitioned into subsets $R_1, \ldots, R_r$ called *parallel classes* where each R_i consists of pairwise disjoint blocks whose union equals the set of all elements V. The BIBD$(9, 12, 4, 3, 1)$ in Example 2 is resolvable.

The BIBD is usually assumed to have $k \geq 3$ since a BIBD with $k = 2$ has a structure of a complete graph (or of a multicomplete graph). However, a resolvable BIBD with $k = 2$ and $\lambda = 1$ is equivalent to a 1-factorization of the complete graph, and is well known to exist if and only if the number of elements (i.e. vertices of the complete graph) is even.

Given two BIBDs $(V, \mathcal{B})$ and $(W, \mathcal{C})$, a mapping $\alpha : V \to W$ such that $\alpha V = W$ and $\alpha \mathcal{B} = \mathcal{C}$ is an *isomorphism*; the two BIBDs are *isomorphic.* An isomorphism from a design to itself is an *automorphism.* The set of all automorphisms of $(V, \mathcal{B})$ forms a group called the *full automorphism group* of $(V, \mathcal{B})$. Any of its subgroups is an *automorphism group* of $(V, \mathcal{B})$.

Exercise 1. Show that any two BIBD$(7, 3, 1)$ are isomorphic.
Exercise 2. Determine the order of the full automorphism group of a BIBD$(7, 3, 1)$.

Groups and the existence of designs are closely related since often in showing the existence of a design a method is utilized by which one assumes the existence of a design with a specified automorphism group. This allows one to select a small basic set of blocks (*the base*) containing representatives of all orbits of blocks under the group in question. The collection $\mathcal{B}$ of all blocks is then obtained by letting the group act on these base blocks.

For example, a (v, k, λ)-design is *cyclic* if it admits a cyclic group of order v as its automorphism group. Alternatively, it is cyclic if it admits an automorphism permuting the elements in a single cycle of length v. The elements of a cyclic design are usually taken as elements of Z_v, with $\alpha : i \to i + 1$ as its cyclic automorphism.

Given a design $(V, \mathcal{B})$, the *element-block incidence graph* of $(V, \mathcal{B})$ or *Levi graph* of $(V, \mathcal{B})$ is a bipartite graph $G(V, \mathcal{B})$ which has as its vertex set $V \cup \mathcal{B}$, and edges joining $x \in V$ with $B \in \mathcal{B}$ exactly when $x \in B$. Two designs $(V, \mathcal{B})$ and $(W, \mathcal{C})$ are isomorphic if and only if the graphs $G(V, \mathcal{B})$ and $G(W, \mathcal{C})$ are isomorphic. The automorphism group of a simple design $(V, \mathcal{B})$ is isomorphic to the automorphism group of the graph $G(V, \mathcal{B})$ (a design is *simple* if it contains no repeated blocks).

Exercise 3. Determine the Levi graph of the $(7, 3, 1)$-BIBD.

Another graph associated with a (v, k, λ)-BIBD is its *block intersection graph* (BIG). Its vertices are the blocks of the BIBD, and two blocks B and B' are adjacent if $B \cap B' \neq \emptyset$. More specifically, in the *i-block intersection graph* B and B' are adjacent if $|B \cap B'| = i$. When $\lambda = 1$, BIG is a strongly regular graph with parameters (v', k', λ, μ).

Exercise 4. Given a BIBD$(v, b, r, k, 1)$, determine the parameters (v', k', λ, μ) of its block intersection graph.

An *isomorphism invariant* is a function I such that $I(V, \mathcal{B}) = I(W, \mathcal{C})$ if $(V, \mathcal{B})$ and $(W, \mathcal{C})$ are isomorphic. An invariant I is *complete* provided $I(V, \mathcal{B}) = I(W, \mathcal{C})$ if and only if $(V, \mathcal{B})$ and $(W, \mathcal{C})$ are isomorphic. No easily computable complete isomorphism invariant is known for BIBDs and none is likely to exist since the isomorphism problem for BIBDs was shown to be graph-isomorphism complete.

A more general type of balanced designs are t-designs. For an integer $t \geq 2$, a $t - (v, k, \lambda)$ design is an ordered pair $(V, \mathcal{B}))$ where V is a v-set of *elements*, and $\mathcal{B}$ is a collection of k-subsets of V called *blocks* such that every t-subset of V is contained in exactly λ blocks. A $t - (v, k, \lambda)$ design with $\lambda = 1$ is a Steiner system $\mathrm{S}(t, k, v)$. A Steiner system $\mathrm{S}(2, 3, v)$ is a Steiner triple system, and an $\mathrm{S}(3, 4, v)$ is a Steiner quadruple system. Thus BIBDs are 2-designs, and BIBDs with $\lambda = 1$ are Steiner 2-designs. Only a finite number of Steiner systems $\mathrm{S}(t, k, v)$ with $t \geq 4$ are known, and none is known for $t \geq 6$. From among the known Steiner systems with larger t, the most "famous" are those associated with the five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, namely $\mathrm{S}(4, 5, 11)$, $\mathrm{S}(5, 6, 12)$, $\mathrm{S}(3, 6, 22)$, $\mathrm{S}(4, 7, 23)$, $\mathrm{S}(5, 8, 24)$.

2. Quasigroups and latin squares. MOLS and orthogonal arrays

A *quasigroup* is a pair (Q, o) where Q is set and "o" is a binary operation on Q such that whenever $a, b \in Q$, there is a unique solution to the equation $a\ o\ x = b$ and to the equation $y\ o\ a = b$. For our purposes, all quasigroups will be finite, and if $|Q| = n$, the quasigroup is of *order* n. A *latin square* of order n is an $n \times n$ array each cell of which contains exactly one of the symbols from an n-set (which is usually taken to be $\{1, 2, \ldots, n\}$) such that each row and each column of the array contains each of the symbols exactly once. Thus a quasigroup of order n can be viewed as a latin square of order n with a headline and a sideline.

A latin square [quasigroup] is *idempotent* if the cell (i, i) contains the symbol i for all i [if $i\ o\ i = i$ for all i]. A latin square [quasigroup] is *commmutative* if cells (i, j) and (j, i) contain the same symbol for all i, j [if $i\ o\ j = j\ o\ i$ for all i, j]. An idempotent commutative quasigroup exists for all odd orders.

A latin square [quasigroup] of even order $2n$ is *half-idempotent* if the cells (i, i) and $(n + i, n + i)$ contain the symbol i for all $i, 1 \leq i \leq n$ [if $i\ o\ i = i$ and $(n + i)\ o\ (n + i) = i$ for all $i, 1 \leq i \leq n$]. A half-idempotent commutative latin square exists for all even orders.

Two latin squares $A = (a_{ij})$ and $B = (b_{ij})$ are *orthogonal* if the n^2 ordered pairs (a_{ij}, b_{ij}) are all distinct. A set of latin squares $A_1, A_2, \ldots, A_r$ are mutually orthogonal if any two are orthogonal. Such a set is termed MOLS, or MOLS(n).

Let $N(n)$ be the largest number t such that there exists a set of t MOLS(n). A first observation is that $N(n) \leq n - 1$. Indeed, if $A_1, A_2, \ldots, A_r$ is a set of MOLS(n), relabel each of the r squares so that the cell $(1, 1)$ is occupied by 1; this does not affect the orthogonality. More generally, let the first row be $1, 2, \ldots, n$. The entries in the cell $(2, 1)$ in the r squares must be mututally different, and also distinct from 1.

Theorem 1. *Let n be a prime power, i.e. $n = p^k$. Then $N(n) = n - 1$, i.e. there exists a set of $n - 1$ MOLS(n).*

Proof. Let $n = p^k$, and let the elements of GF(n) be $b_1, b_2, \ldots, b_n$, with b_1 the multiplicative identity, and b_n the additive identity. For $t = 1, 2, \ldots, n - 1$, define the $n \times n$ array $A^{(t)} = (a_{ij}^{(t)})$ by $a_{ij}^{(t)} = (b_t \times b_i) + b_j$.

Exercise 5. 1. Show that for $t = 1, \ldots, n - 1$, the array $A^{(t)}$ defined above is a latin square.

2. Show that for $t \neq u$, the latin squares $A^{(t)}$ and $A^{(u)}$ are orthogonal.

MacNeish's Theorem. *If there exists a set of r MOLS(m) and a set of r MOLS(n) then there exists a set of r MOLS($m.n$).*

Proof. Take the Kronecker product of $A^{(i)}, B^{(i)}$ for $i = 1, 2, \ldots, r$ where $A^{(1)}, \ldots, A^{(r)}$ and $B^{(1)}, \ldots, B^{(r)}$ are MOLS(m) and MOLS(n), respectively.

Corollary. *If $n = p_1^{\alpha_1}.p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ is the prime power decomposition of n then $N(n) \geq min_i(p^{\alpha_i} - 1)$.*

To determine the value of $N(n)$ is one of the foremost problems in combinatorial theory. It is known that $N(n) \geq 2$ for all $n \neq 2, 6$, $N(n) \geq 3$ for all $n \neq 2, 3, 6$ and possibly 10. It is not known at present whether there exist or not three mutually orthogonal latin squares of order 10. Many other lower bounds on the number of MOLS(n) are known when n is not a prime power.

Two ordered n^2-tuples $(a_1, a_2, \ldots, a_{n^2})$ and $(b_1, b_2, \ldots, b_{n^2})$ of elements from an n-set are *orthogonal* if the ordered pairs (a_i, b_i), $i = 1, 2 \ldots, n^2$, contain every possible ordered pair exactly once.

An *orthogonal array* OA(s, n) of order n and depth s is an $s \times n^2$ array with entries from an n-set N (more often than not $N = \{1, 2, \ldots, n\}$) with the property that any two rows are orthogonal.

Given a set of k MOLS(n), $L_1, \ldots, L_k$, form, for any ordered pair (i, j), $i, j \in \{1, 2, \ldots, k\}$, the column $(i, j, L_1(ij), \ldots, L_k(ij))^T$. The result is an OA$(k + 2, n)$. Conversely, given an OA$(k + 2, n)$, one can obtain a set of k MOLS(n).

Exercise 6. Construct a set of 3 MOLS(4) and use it to obtain an OA(5, 4).

3. Affine and projective planes

Some of the origins of modern combinatorial design theory can be traced to examples from finite geometry. With *points* and *lines* taken as undefined elements, a finite geometry is one with a finite number of points. It is a *projective plane* if it satisfies the following axioms:

P1. Two distinct points are contained in exactly one line.

P2. Any two distinct lines intersect in a unique point.

P3. There exist four points no three of which are collinear (i.e. lie on the same line).

Given a finite projective plane, there exists a number n called its *order* such that any line contains $n + 1$ points, each point is contained in $n + 1$

lines, and the total number of points and also the total number of lines equals $n^2 + n + 1$.

Example 1 above is, in effect, a projective plane of order 2 (just call the elements points, and the blocks lines). This is the smallest possible projective plane. Another example is provided by a BIBD$(13, 4, 1)$ whose elements are the elements of Z_{13} and the blocks are given by
$B_i = \{\{i, i+1, i+3, i+9\}\}, i \in Z_{13}$. More generally, the following holds.

For each prime power q, there exists a projective plane of order q.

If we take the points as elements and the lines as blocks, a finite projective plane is a symmetric BIBD with parameters $v = b = n^2 + n + 1$, $r = k = n + 1$, $\lambda = 1$. But also conversely, given a BIBD with parameters $(v, k, \lambda) = (n^2 + n + 1, n + 1, 1)$, it is a projective plane since the axioms are clearly satisfied.

Many further examples of designs are provided by *projective spaces.* Any finite projective space of dimension 3 or higher is obtained as follows: In a vector space V of dimension $d + 1$ over the finite field F_q, take as points the 1-dimensional subspaces and as lines the 2-dimensional subspaces of V. This projective space is usually denoted by PG(d, q) and has $v = \frac{q^{d+1}-1}{q-1} = q^d + q^{d-1} + \cdots + q + 1$ elements, $k = q + 1$ points on a line, and $\lambda = 1$. However, not all BIBDs with these parameters are projective spaces.

The smallest example of a "proper" (i.e. 3-dimensional) projective space is given by PG$(3, 2)$. It has 15 points and 35 lines, each containing three points, and as a design is a $(15, 3, 1)$-BIBD. It is also a Steiner triple system (see below) of order 15.

A finite *affine plane* satisfies the following axioms:

A1. Two distinct points are contained in exactly one line.

A2. For any point P not on a line l there is exactly one line containing P that has no common point with l.

A3. There exist three noncollinear points.

Axiom A2 is the euclidean parallel axiom. This naturally defines the relation of *parallelism* on the set of lines; equivalence classes of parallelism are *parallel classes* each of which partitions the set of points.

The number of points on a line is the order n of the affine plane. The number of points in an affine plane of order n is n^2, the number of lines is $n^2 + n$, and the number of parallel classes is $n + 1$ which is also the number of lines containing a given point. As a design, an affine plane is an $(n^2, n, 1)$-BIBD, and conversely, any BIBD with the above parameters is an affine plane. The BIBD$(9, 12, 4, 3, 1)$ from Example 2 is, in effect, an affine plane of order 3.

If we recast affine and projective planes in terms of BIBDs, then an affine plane of order n is the residual design of a projective plane. Also the converse, and more, holds as the following theorem shows.

Theorem 2. *The following are equivalent:*

(i) There exists an affine plane of order n.

(ii) There exists a projective plane of order n.

(iii) There exists a set of $n-1$ MOLS(n).

(iv) There exists an $OA(n+1, n)$.

Proof. (i) → (iii). Let an affine plane of order n be given, with its $n^2 + n$ lines partitioned into $n+1$ parallel classes having n lines each. Designate arbitrarily two parallel classes as F_r, F_c and the remaining parallel classes as $F_1, F_2, \ldots, F_{n-1}$. Number the lines in each parallel class arbitrarily from 1 to n; the numbering in F_r is that of the rows of the square, in F_c of the columns of the square. A point of the affine plane is on one line of F_r and on one line of F_c, so is associated with a particular cell of the square. Write (i, j) for the point in ith row and jth column. For each of the parallel classes $F_1, \ldots, F_{n-1}$, we construct a latin square as follows. Let F_u be one of these parallel classes containing lines $L^u_1, \ldots, L^u_n$. From F_u construct a square A_u by inserting the number x in the (i, j) cell if the point associated with this cell (being on the ith line of F_r and jth line of F_c) lies on the xth line L^u_x of the parallel class F_u. Since every point lies on exactly one line of F_u, there is exactly one number in each cell of A_u. A line of F_r (of F_c, respectively) intersects each line of F_u exactly once, and so any row (or column) of A_u contains each of $1, \ldots, n$ exactly once. Thus A_u is a latin square of order n.

Let $A_u = (a_{ij})$, $A_w = (b_{ij})$. If we had $a_{i_1,j_1} = a_{i_2,j_2}$ and also $b_{i_1,j_1} = b_{i_2,j_2}$ (in violation of the "two fingers" rule) this would mean that the points (i_1, j_1) and (i_2, j_2) both lie on the line L^u_a of F_u and on the line L^U_b of F_w, contrary to axiom A1. So the ordered pairs (a_{ij}, b_{ij}), $i, j = 1, 2, \ldots, n$ must be all distinct, i.e. A_u and A_w are orthogonal.

(iii) → (i). Consider each cell (i, j) as a point and form families of lines $F_r, F_c, F_1, \ldots, F_{n-1}$ where the point (i, j) is on the ith line of F_r, on the jth line of F_c, and on the xth line of F_u, $u = 1, 2, \ldots, n-1$, if the (i, j)-cell of the latin square A_u contains x. This yields $n+1$ parallel classes of lines, each with n lines.

The equivalence of (iii) and (iv) has been noted above.

4. Symmetric designs

In the negative direction, we have the Bruck-Ryser-Chowla theorem which states that if a symmetric (v,k,λ)-BIBD exists then if v is odd, the equation $z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ has a solution in integers x, y, z not all zero.

For example, BIBD$(43,7,1)$ (a projective plane of order 6) cannot exist since the condition of the Bruck-Ryser-Chowla Theorem reduces here to $z^2 + y^2 = 6x^2$ which has no solution in integers x, y, z not all zero.

In fact, for $\lambda = 1$ the Bruck-Ryser-Chowla Theorem reduces to the following necessary condition for the existence of a symmetric $(v,k,1)$-BIBD i.e. a projective plane of order $n = k-1$:

A necesary condition for the existence of a finite projective plane of order n is that when $n \equiv 1, 2 \ (mod\ 4)$, there exist integers x, y such that $n = x^2 + y^2$.

This implies that for infinitely many numbers n a projective plane of order n cannot exist, such as $n = 6, 14, 21, 22, \ldots$. The smallest order which is not covered by this theorem nor is a prime power is 10, however, it has been proved that there exists no projective plane of order 10, i.e. a symmetric $(111, 11, 1)$-BIBD. Currently, the smallest order for which the existence of a projective plane is undecided is 12.

Symmetric designs with $\lambda = 2$ are called *biplanes*. In a biplane, $v = \binom{k}{2} + 1$. Biplanes are known to exist for only 6 values of v. Similarly, symmetric designs with $\lambda = 3$ are known to exist only for 6 values of v. A longstanding conjecture that for any $\lambda > 1$ there exists only a finite number of symmetric designs remains open.

5. Difference sets and difference families

A set of k residues $D = \{a_1, \ldots, a_k\}$ modulo v is a cyclic (v,k,λ)-difference set if for every $d \not\equiv 0 \ (mod\ v)$ there are exactly λ ordered pairs $(a_i, a_j),\ a_i, a_j \in D$ such that $a_i - a_j \equiv d \ (mod\ v)$. A more general type of a difference set in an abelian group is defined similarly.

For example, $\{0,1,3\}$ is a $(7,3,1)$-difference set, $\{0,1,3,9\}$ is a $(13,4,1)$-difference set, $\{0,1,4,14,16\}$ is a $(21,5,1)$- difference set, $\{0,1,3,8,12,18\}$ is a $(31,6,1)$-difference set, $\{0,2,3,4,8\}$ is a $(11,5,2)$-difference set, $\{0,1,2,4, 5,8,10\}$ is a $(15,7,3)$-difference set. All these difference sets are cyclic.

Theorem 3. *A set of k residues $D = \{a_1, \dots, a_k\}$ modulo v is a (v, k, λ)-difference set if and only if the sets $B_i = \{a_1 + i, \dots, a_k + i\}$ modulo v, $i = 0, 1, \dots, v-1$ form a cyclic (v, k, λ)-BIBD.*

A family $\mathcal{D} = \{D_1, \dots, , D_s\}$ where $D_i = \{a_1^i, a_2^i, \dots, a_k^i\}$ is a $(v, k, \lambda; s)$ difference family if for every $d \not\equiv 0$ $(mod\ v)$ there are exactly λ ordered pairs (a_p^r, a_q^r) such that $a_p^r - a_q^r \equiv d$ $(mod\ v)$, $r \in \{1, 2, \dots, s\}$. For example, $\{\{0, 1, 4\}, \{0, 2, 7\}\}$ is a $(13, 3, 1; 2)$-difference family.

Any $(v, k, \lambda; s)$-difference family gives rise to a cyclic (v, k, λ)-BIBD. This BIBD will have s block orbits under the action of the cyclic group, each consisting of v blocks. So, for example, the $(13, 3, 1; 2)$-differencce family given above yields a cyclic $(13, 3, 1)$-BIBD whose 26 blocks fall into two orbits, each with 13 blocks.

Theorem 4. *Let v be a prime power, $v = 6t + 1 = p^n$, p a prime. Let x be a primitive element of GF(p^n). Then $\{\{x^i, x^{2t+i}, x^{4t+i}\} : i = 0, 1, \dots, t-1\}$ is a $(6t + 1, 3, 1; t)$-difference family.*

Proof. Since x is a primitive element of GF(p^n), we have $x^{6t} = 1$, thus $(x^{3t} - 1)(x^{3t} + 1) = 0$, and since $x^{3t} \neq 1$, we have $x^{3t} + 1 = 0$. Also $x^{2t} - 1 \neq 0$ so let s be determined by $x^{2t} - 1 = x^s$. Moreover, $-(x^{2t} - 1) = x^{s+3t}$ (since $x^{3t} = -1$), and $x^{s+4t} = x^{4t}(x^{2t} - 1) = 1 - x^{4t} = -(x^{4t} - 1)$. The 6 differences arising from the set $\{x^0, x^{2t}, x^{4t}\}$ are $\pm(x^{2t} - 1), \pm(x^{4t} - 1), \pm(x^{4t} - x^{2t})$ which is the same as $x^s, x^{s+t}, x^{s+2t}, x^{s+3t}, x^{s+4t}, x^{s+5t}$. It follows that the differences yielded by all sets of the difference family are $x^{s+i}, x^{s+i+t}, x^{s+i+2t}, x^{s+i+3t}, x^{s+i+4t}, x^{s+i+5t}$, $i = 0, 1, \dots, t-1$, that is, all $x^j, j = 0, 1, \dots, t-1$, meaning that every nonzero difference in the additive group of GF(p^n) occurs exactly once. □

The idea of $(v, k, \lambda; s)$-difference family has been extended by R.C. Bose [B] to form a basis of a method that he called the *method of pure and mixed differences.*

Let G be an additive abelian group, let T be a t-set, and consider the set $V = G \times T$. For two elements $(x, i) \neq (y, j)$ of V, the differences arising from this pair may be of two kinds: (i) when $i = j$, we have *pure* differences $\pm(x - y)$ of class i , and (ii) when $i \neq j$, we have *mixed* differences $\pm(x - y)$ of class ij. A pure difference of any class may equal any nonzero element of G while a mixed difference may equal any element of G, including zero.

Suppose now that there exists a system of k-sets $D_1, \ldots, D_s$ such that every nonzero element of G occurs exactly λ times as a pure difference of class i among the elements of the $D_1, D_2, \ldots, D_s$ for all $i \in T$, and also every element of G occurs exactly λ times as a mixed difference of class ij among the elements of $D_1, \ldots, D_s$ for all $i, j \in T$, $i \neq j$. Then the sets $D_1, \ldots, D_s$ form a *basis* of a (v, k, λ)-BIBD, $(V, \mathcal{D})$, where $\mathcal{D} = \{D_j + g : g \in G, j = 1, \ldots, s\}$ (here one takes obviously $x_j + g = (x + g)_j$).

The above construction is sometimes extended by adding one "infinite" point and "infinite" difference(s).

Example 4. Let G be the cyclic group of order 7. A basis for a $(21, 3, 1)$-BIBD is given by the sets $\{0_1, 1_1, 2_2\}, \{0_1, 2_1, 5_2\}, \{0_1, 3_1, 2_3\}, \{0_2, 1_2, 6_3\}$, $\{0_2, 2_2, 3_1\}, \{0_2, 3_2, 4_3\}, \{0_3, 1_3, 5_2\}, \{0_3, 2_3, 4_1\}, \{0_3, 3_3, 6_1\}, \{0_1, 0_2, 0_3\}$.

Here, as is customary, we write x_i instead of (x, i). It is readily verified that every pure difference $\pm 1, \pm 2, \pm 3$ of class $1, 2, 3$ occurs exactly once, and every mixed difference $0, \pm 1, \pm 2, \pm 3$ of classes $12, 13, 23$ occurs exactly once, so the above sets do indeed form a basis for a $(21, 3, 1)$-BIBD.

Example 5. Let G be the cyclic group of order 5. A basis for a $(21, 3, 1)$-BIBD with the set of elements $V = (Z_5 \times \{1, 2, 3, 4\}) \cup \{\infty\}$ is given by the 14 sets $\{\infty, 0_1, 0_2\}, \{\infty, 0_3, 0_4\}, \{0_1, 1_1, 3_2\}, \{0_1, 2_1, 1_2\}, \{0_1, 0_3, 1_4\}$, $\{0_1, 1_3, 3_4\}, \{0_1, 3_3, 2_4\}, \{0_2, 1_2, 2_3\}, \{0_2, 2_2, 1_4\}, \{0_1, 2_3, 4_3\}, \{0_2, 3_3, 4_3\}$, $\{0_1, 0_4, 4_4\}, \{0_2, 0_4, 2_4\}, \{0_2, 0_3, 3_4\}$.

Similarly as above, one can verify that every pure difference $\pm 1, \pm 2$ of class $1, 2, 3$, or 4 occurs exactly once, and every mixed difference $0, \pm 1, \pm 2$, $\pm 3, \pm 4$ occurs exactly once, as does every "infinite" difference, even though the verification is somewhat more tedious.

6. Group divisible designs and pairwise balanced designs; transversal designs

Relaxing some of the conditions in the definition of BIBDs leads to different types of designs which were originally thought to be only auxiliary but have quickly attained life on their own. Relaxing the requirement that all blocks be of the same size leads to the notion of *pairwise balanced* designs.

Let λ be a positive integer and let K be a set of positive integers. A pairwise balanced design $\mathrm{PBD}_\lambda(v, K)$ is a pair $(V, \mathcal{B})$ where V is a v-set, $\mathcal{B}$ is a collection of subsets of V called *blocks*, and K is the set of *block* *sizes* such that the cardinality of each block belongs to K and every pair of distinct elements belongs to exactly λ blocks.

Thus in a pairwise balanced design (PBD), the requirement of pairwise balance is preserved but the blocks are allowed to be of different sizes. The index λ is usually omitted when $\lambda = 1$, and one writes just PBD(v, K). Blocks of size 2 are usually permitted. PBDs with $\lambda = 1$ are sometimes called *linear spaces* (or 2-*partitions*).

Example 6. Let $V = \{1, 2, 3, 4, 5, 6\}$, $\mathcal{B} = \{\{1, 2, 3, 4\}, \{4, 5, 6\}, \{1, 5\}, \{1, 6\}, \{2, 5\}, \{2, 6\}, \{3, 5\}, \{3, 6\}\}$. Then $(V, \mathcal{B})$ is a PBD$(6, \{2, 3, 4\})$ (with $\lambda = 1$).

For a positive integer λ and K and G sets of positive integers, a *group divisible* design of order v and index λ, GDD$_\lambda(v, K, G)$ is an ordered triple $(V, \mathcal{G}, \mathcal{B})$ where V is a v-set, $\mathcal{G}$ is a partition of V into *groups* whose sizes belong to G, and $\mathcal{B}$ is a collection of subsets called *blocks* whose cardinalities belong to the set of block sizes K such that every pair of distinct elements of V is contained in exactly λ blocks or in one group (but not both), and $|\mathcal{G}| \geq 2$. Subscript λ is usually suppressed when $\lambda = 1$.

Given a GDD$_\lambda(V, K, G)$ with a_i groups of size g_i, $i = 1, \dots, s$ (so that $\Sigma_{i=1}^{s}\ \alpha_i g_i = v$), the GDD is said to be of *type* $g_1^{a_1} g_2^{a_2} \dots g_s^{a_s}$. When $K = \{k\}$ and $\lambda = 1$, one speaks of a k-GDD.

Example 7. A 3-GDD of type 2^4 has as its groups $\{0, 4\}, \{1, 5\}, \{2, 6\}, \{3, 7\}$ and as its blocks $\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 0\}, \{6, 7, 1\}, \{7, 0, 2\}$.

A special case of a GDD is a *transversal design* TD$_\lambda(n, r)$. This is a GDD$_\lambda(rn; r, n)$, that is, there are r groups, each with n elements, all blocks have cardinality r, and thus any group and any block have exactly one element in common. Again, when $\lambda = 1$, one writes only TD(n, r).

Some of examples of transversal designs are:

1. Take an affine plane of order n, declare one of its parallel classes to be the groups and the remaining lines to be blocks. This gives a TD(n, n).

2. Take a projective plane of order n and remove one point, say x. Declare all lines containing x, with x removed, to be the groups and the remaining lines to be the blocks. This gives a TD$(n, n + 1)$.

3. Take a latin square $L = (A_{ij})$ of order n, take as the three groups the rows, the columns, and the entries of L, respectively. Take as blocks the sets $\{r_i, c_j, a_{ij}\}$ where a_{ij} it the entry in row r_i and column c_j of L. This gives a TD$(n, 3)$.

Theorem 5. *A transversal design TD(n, r) exists if and only if there exists a set of $r-2$ MOLS(n).*

A TD(n,r) is *resolvable* if its blocks can be partitioned into parallel classes. A resolvable TD(n,r) is denoted by RTD(n,r).

Theorem 6. *A resolvable trasnversal design RTD(n, r) exists if and only if there exists a set of $r-1$ MOLS(n).*

*　　　　*　　　　*

For a set of positive integers K, let $\alpha(K) = \gcd\{k-1 : k \in K\}$ and $\beta(K) = \gcd\{k(k-1) : k \in K\}$. Then the necessary conditions for the existence of a PBD(v,K) are

$v - 1 \equiv 0 \ (mod\ \alpha(K))$ and $v(v-1) \equiv 0 \ (mod\ \beta(K))$.

A set K of positive integers is *PBD-closed* if the existence of a PBD(v,K) implies that $v \in K$. For K a set of positive integers, the PBD-*closure* of K is the set $B(K) = \{v : \text{there exists a PBD}(v,K)\}$.

The following theorem due to Richard Wilson [W] states that the necessay conditions for the existence of a PBD(v,K) are asymptotically sufficient.

Theorem 7. *Let K be a PBD-closed set. Then there exists a constant $v_0 = v_0(K)$ such that if $v > v_0$ and v satisfies the above necessary conditions then there exists a PBD(v, K).*

II. STEINER TRIPLE SYSTEMS

1. Existence

Steiner triple systems are BIBDs with $k = 3$ and $\lambda = 1$. They are the smallest nontrivial instance of BIBDs, as BIBDs with $k = 2$ are trivial (except when considering resolvability or other additional properties). The arithmetic necessary conditions reduce to $v \equiv 1 \ (mod\ 2)$, $v(v-1) \equiv 0 \ (mod\ 6)$ whence $v \equiv 1$ or $3 \ (mod\ 6)$, thus only one parameter v remains. The abbreviation commonly used is STS(v). The BIBDs in Examples 1 and 2 are STS(7) and STS(9), respectively.

The first proof that the necessary condition above is also sufficient for the existence of STSs was provided by Kirkman in 1847. The simplest currently known *direct* and *recursive* proofs of this fact are as follows.

The Bose construction. Let (Q, o) be any idempotent commutative quasigroup of order $2n+1$ where $Q = \{1, 2, \ldots, 2n+1\}$. Let $V = Q \times Z_3$, and let $\mathcal{B}$ consist of two types of triples:

(1) $\{x_0, x_1, x_2\}, x \in Q$

(2) $\{x_i, y_i, (x\ o\ y)_{i+1}\}$, $x, y \in Q, x \neq y$, $i \in Z_3$.

Then $(V, \mathcal{B})$ is an STS$(6n+3)$.

To see this, first count the number of triples. There are $2n+1$ triples in (1), and $\binom{2n+1}{2}$ choices for x and y, with three triples corresponding to each such choice in (2). So $|\mathcal{B}| = 2n+1+3\binom{2n+1}{2} = (2n+1)(3n+1)$ which is the correct number of triples in any STS$(6n+3)$. It only remains to be shown that each pair of distinct elements is contained in at least one triple. Let a_j, b_k be such a pair. If $a = b$ then $\{a_1, a_2, a_3\}$ is a triple in (1) containing a_j and a_k. If $j = k$ then $a \neq b$ and thus $\{a_j, b_j, (a\ o\ b)_{j+1}\}$ is a triple in (2) containing the pair (a_j, b_j). Finally, let $a \neq b$ and $j \neq k$; assume w.l.o.g. $j = 1$ and $k = 2$. Since (Q, o) is a quasigroup, there must exist $p \in Q$ such that $a\ o\ p = b$. Since (Q, o) is idempotent and $a \neq b$, it must be that $p \neq a$. Therefore $\{a_1, p_1, (a\ o\ p)_2 = b_2)$ is a triple in (2) containing a_1 and b_2.

The Skolem construction. Let (Q, o) be any half-idempotent commutative quaasigroup of order $2n$ where $Q = \{1, 2, \ldots, 2n\}$. Let $V = \{\infty\} \cup (Q \times \{Z_3\}$, and let $\mathcal{B}$ consist of three types of triples:

(1) $\{x_0, x_1, x_2\}, 1 \leq x \leq n$,

(2) $\{\infty, (n+x)_i, x_{i+1}\}$, $1 \leq x \leq n$, $i \in Z_3$,

(3) $\{x_i, y_i, (x\ o\ y)_{i+1}\}, x, y \in Q, x \neq y, i \in Z_3$.

Then $(V, \mathcal{B})$ is an STS$(6n+1)$.

Bose and Skolem constructions together yield a simple direct proof of the existence of STSs.

As for recursive constructions (constructing larger designs from smaller designs), the first result shows that if there exists an STS(v) and an STS(w) then there exists an STS$(v.w)$. There is a simple combinatorial proof of this but this is also a direct consequence of some algebraic considerations (see below).

In what follows we need a simple auxiliary device which is however interesting on its own. A 1-*factorization* of the complete graph K_n is a partition of the edges of K_n into 1-factors (=perfect matchings). One-factorizations of K_n are often written as pairs $(X, \mathcal{F})$ where X is the vertex set of K_n and $\mathcal{F} = \{F_1, F_2, \ldots, F_{n-1}\}$ is the set of 1-factors. More about

1-factorizations will be said later. At this point we just observe that it is easy to find a 1-factorization of K_n by using an idempotent commutative quassigroup of order $n-1$ (n must be even, so the quasigroup order $n-1$ is odd). Let (Q, o) be such an idempotent commutative quasigroup of order $n-1$ where $Q = \{1, 2, \ldots, n-1\}$. For each $i \in Q$, let $F_i = \{\{i, n\}\} \cup \{\{x \; o \; y\} : x \; o \; y = y \; o \; x = i\}$. Then $\mathcal{F} = \{F_1, F_2, \ldots, F_{n-1}\}$ is a 1-factorization of K_{n+1} on $X = \{1, 2, \ldots, n\}$.

The $v \to 2v+1$ **construction**. Let $(V, \mathcal{B})$ be an STS(v) and let $(X, \mathcal{F})$ be a 1-factorization of K_{v+1} on X where $X \cap V = \emptyset$ and $\mathcal{F} = \{F_1, \ldots, F_v\}$. Let $W = V \cup X$ and let $\mathcal{C}_i = \{\{i, x, y\} | \{x, y\} \in F_i\}$, $\mathcal{C} = \cup_{i \in V} \; \mathcal{C}_i$. Then $(W, \mathcal{B} \cup \mathcal{C})$ is an STS($2v+1$) containing $(V, \mathcal{B})$ as a subsystem.

The $v \to 2v+7$ **construction**. Let $(V, \mathcal{B})$ be an STS(v) ($v \geq 7$), let X be a set, $|X| = v+7$, and let $\mathcal{F} = \{F_1, \ldots, F_v\}$ be a set of 1-factors in the complete graph K_{v+7} on X which together with a set T of $v+7$ triples forms a partition of the edges of K_{v+7}. Let $W = V \cup X$, let $\mathcal{C}_i = \{\{i, x, y\} | \{x, y\} \in F_i\}$, $\mathcal{C} = \cup_{i \in V} \mathcal{C}_i$. Then $(W, \mathcal{B} \cup \mathcal{C} \cup T)$ is an STS($2v+7$) containing $(V, \mathcal{B})$ as a subsystem.

What is needed to validate this construction is to show that the edges of the complete graph K_{v+7} (where $v+7$ is an even number) can be indeed partitioned into $v+7$ triples and v one-factors. There are several results from which this would follow, including the Stern-Lenz Lemma [SL], or the Chetwynd-Hilton result on 1-factorability of regular graphs of sufficiently high degree [CH].

Starting now with Steiner triple systems of orders 3, 9, and 13 and applying the $2v+1$ and $2v+7$ constructions recursively proves the existence of STSs of all admissible orders.

The number of nonisomorphic STSs increases rapidly with order. If $N(v)$ is the number of nonisomorphic STS(v) then for sufficiently large v, we get $N(v) = v^{v^2(\frac{1}{6}+o(1))}$. The complexity of deciding the isomorphism of STSs is unknown. The best known algorithm is subexponential.

2. Cyclic STSs

An STS(v) is *cyclic* if it admits an automorphism consisting of a single cycle of length v. The blocks of such an STS can be presented in a compact form by listing one representative of each orbit of blocks under a cyclic automorphism α. The elements of a cyclic STS(v) may be assumed to be Z_v. Thus, for example, the blocks of (a design isomorphic to) the STS(7) from Example 1 may be written as $\{i, i+1, i+3\}$, $i \in Z_7$, or, as is more customary, as $\{0,1,3\}$ *mod* 7, or even more simply 0 1 3 *mod* 7.

Exercise 7. Show that there exists no cyclic STS(9).

The existence of cyclic STSs is proved via solutions to two Heffter's difference problems; the latter can in turn be obtained via Skolem and related sequences.

First Heffter's difference problem. (I.HDP(n)) For any natural k, partition the set of $3k$ integers $\{1,2,\ldots,3k\}$ into k ordered triples $(a_i, b_i, c_i), i = 1,2,\ldots,k$ such that for all $i = 1,2,\ldots,k$, either (1) $a_i+b_i = c_i$ or (2) $a_i + b_i + c_i = 6k+1$.

Second Heffter's difference problem. (II.HDP(n)) For any natural k, partition the set of $3k$ integers $\{1,2,\ldots,2k,2k+2,\ldots,3k+1\}$ into k ordered triples $(a_i, b_i, c_i), i = 1,2,\ldots,k$ such that for all $i = 1,2,\ldots,k$, either (1) $a_i + b_i = c_i$, or (2) $a_i + b_i + c_i = 6k+3$.

Lothar Heffter formulated these problems in 1890s. Rose Peltesohn provided the first solution to both Heffter's difference problems in 1939 by using a recursive method. A different, direct, proof can be obtained by using so-called Skolem sequences and similar sequences.

Given a solution to the First Heffter's difference problem, i.e. the ordered triples $\{(a_i, b_i, c_i) : i \in \{1,2,\ldots,n\}$, form triples $\{\{0, a_i, a_i+b_i\} : i \in \{1,2,\ldots,n\}\}$. These are base triples of a cyclic STS($6n+1$). Similarly, given a solution to II.HDP(n), the triples $\{\{0, a_i, a_i+b_i\} : i \in \{1,2,\ldots,n\}\}$ together with the triple $\{0, 2n+1, 4n+2\}$ form a set of base blocks of a cyclic STS($6n+3$).

Thus the problem of proving the existence of cyclic STS(v) for $v \equiv 1$ or 3 (*mod* 6) is reduced to finding solutions to I.HDP and to II.HDP. The latter can in turn be reduced to finiding certain integer sequences.

In 1957, Thoralf Skolem [Sk], [Sk1] defined a sequence (which today carries his name) for the expressed purpose of constructing cyclic Steiner triple systems. A sequence of length $2n$, say, $(a_1, a_2, \ldots, a_{2n})$, is a *Skolem sequence* of order n if it satisfies

1. for every $k \in \{1, 2, \ldots, n\}$, there are exactly two elements a_i, a_j of the sequence such that $a_i = a_j = k$, and

2. if $a_i = a_j$, $i < j$, then $j - i = k$.

Skolem sequences are often given as a collection of ordered pairs $\{(a_i, b_i) : 1 \le i \le n\}$ where $\cup_{i=1}^{n}\{a_i, b_i\} = \{1, 2, \ldots, n\}$.

For example, 42324311 or $\{(7,8), (2,4), (3,6), (1,5)\}$ is a Skolem sequence of order 4.

Exercise 8. Show that $n \equiv 0$ or $1(mod\ 4)$ is a necessary condition for the existence of a Skolem sequence of order n.

An *extended Skolem sequence* of order n is a sequence of length $2n + 1$, say, $\{a_1, a_2, \ldots, a_{2n+1}\}$ satisfying conditions 1. and 2. above, and also
3. there is exactly one a_i such that $a_i = 0$.

For example, 5641154623203 or, equivalently, $\{(4,5), (9,11), (10,13), (3,7), (1,6), (2,8)\}$ is an extended Skolem sequence of order 6.

An extended Skolem sequence with $a_{2n} = 0$ is a *hooked* Skolem sequence. The example above is that of a hooked Skolem sequence.

Let $\{(a_i, b_i) : i = 1, \ldots, n\}$ be a Skolem sequence or a hooked Skolem sequence of order n. Then the set of ordered triples $\{(i, a_i + n, b_i + n) : i = 1, 2, \ldots, n\}$ is a solution of the first Heffter's difference problem. An extended Skolem sequence with zero in the middle (i.e. $(n + 1)$st) position can be used in a similar way to obtain a solution to the second Hefffter's difference problem.

3. STSs as quasigroups

Let (V, o) be an idempotent totally symmetric quasigroup, i.e. a quasigroup satisfying

(i) $x\ o\ x = x$ (the idempotent law)

(ii) $x\ o\ y = y\ o\ x$ (the symmetry law), and

(iii) $x\ o\ (x\ o\ y) = y$ (the law of total symmetry).

Define $\mathcal{B} = \{\{x, y, x\ o\ y\} : x, y \in V, x \neq y\}$. Then $(V, \mathcal{B})$ is a Steiner triple system.

Conversely, given an STS(v), $(V, \mathcal{B})$, define on V a binary operation "o" by

(i) for all $x \in V, \quad x \ o \ x = x$,

(ii) for all $x, y \in V, x \neq y, \quad x \ o \ y = z$ where $\{x, y, z\} \in \mathcal{B}$ is the triple containing the pair $\{x, y\}$.

Then (V, o) is an idempotent totally symmetric quasigroup (an ITS quasigroup). Such quasigroup is usually called a *Steiner quasigroup* (or a squag). Thus Steiner quasigroups form an *equational class* or a *variety* of algebras, and as such are closed under taking subalgebras, cartesian products and homomorphic images.

It is sometimes useful to consider *Steiner loops.*

Lert (Q, o, e) be a loop (a quasigroup with a unit element e) satisfying the identities

(i) $x \ o \ e = x$,

(ii) $x \ o \ y = y \ o \ x$, and

(iii) $x \ o \ (x \ o \ y) = y$.

Define $V = Q \setminus \{e\}$, and $\mathcal{B} = \{\{x, y, x \ o \ y\} : x, y \in V', x \neq y\}$. Then $(V', \mathcal{B})$ is a Steiner triple system.

Conversely, given an STS(v), $(V, \mathcal{B})$, define on $Q = V \cup \{e\}$ a binary operation "o" by

(i) for all $x \in V, \ x \ o \ x = x$; $e \ o \ e = e$,

(ii) for all $x \in V, \ x \ o \ e = e \ o \ x = x$, and

(iii) (ii) for all $x, y \in V, x \neq y, \ x \ o \ y = z$ where $\{x, y, z\} \in \mathcal{B}$ is the triple containing the pair $\{x, y\}$.

Then (Q, o, e) is a totally symmetric loop, called Steiner loop. Steiner loops also form a variety. The usefulness of this representation is readily seen from the following example: to an STSv correspond both, the Steiner quasigroup of order v and the Steiner loop of order $v + 1$. But the direct product of two Steiner quasigroups of orders m and n corresponds to an STS($m.n$) while the direct product of two Steiner loops of orders $m+1$ and $n + 1$ corresponds to an STS($mn + m + n$).

One further important operation on quasigroups is the so-called *singular direct product.* It is defined as follows.

Let $(V, \square)$ be an idempotent quasigroup, (Q, o) a quasigroup containing a subquasigroup P, let $P' = Q \setminus P$, and let $(P', *)$ be a quasigroup ($*$ and o need not be related). On the set $P \cup (P' \times V)$ define a binary operation $\otimes$ as follows.

(1) $x \otimes y = x\ o\ y$ if $x, y \in P$,
(2) $x \otimes (x', v) = (x\ o\ x', v)$ where $x \in P,\ x' \in P', v \in V$;
(3) $(x', v) \otimes x = (x'\ o\ x, v)$ where $x \in P,\ x' \in P', v \in V$;
(4) $(x', v) \otimes (y', v) = x'\ o\ y'$ if' $x'\ o\ y' \in P$
$\qquad = (x'\ o\ y', v)$ if $x'\ o\ y' \in P'$;
(5) $(x', v) \otimes (y', w) = (x' * y', v \Box w)$, $v \neq w$.

The qroupoid $V \times Q(P, P', \times)$ defined above is a quasigroup called the singular direct product of V and Q.

4. Kirkman triple systems

A *Kirkman triple system* (KTS) $(V, \mathcal{B}, \mathcal{R})$ is a structure where $(V, \mathcal{B})$ is an STS(v) and $\mathcal{R} = \{R_1, \ldots, R_{\frac{v-1}{2}})$ is a *resolution* of the triples of $\mathcal{B}$ into *parallel classes* (or resolution classes) each of which partitions V. The underlying STS $(V, \mathcal{B})$ is *resolvable.* It is possible for a resolvable STS to admit several nonisomorphic KTSs.

Example 2 contains a resolvable STS(9) whose resolution is unique. The famous "Problem of 15 schoolgirls" formulated by Rev. T.P. Kirkman in the 1840s asks whether there exists a resolvable STS(15). An example of a KTS(15) with $V = Z_{15}$ is the following:

R_1 : 0 1 2 3 9 13 4 7 12 5 8 14 6 10 11
R_2 : 0 3 4 1 11 13 2 8 9 5 10 12 6 7 14
R_3 : 0 5 6 1 7 9 2 11 14 3 8 12 4 10 13
R_4 : 0 7 8 1 4 6 2 12 13 3 10 14 5 9 11
R_5 : 0 9 10 1 12 14 2 4 5 3 7 11 6 8 13
R_6 : 0 11 12 1 8 10 2 3 6 4 9 14 5 7 13
R_7 : 0 13 14 1 3 5 2 7 10 4 8 11 6 9 12.

The underlying STS(15) of the above KTS is PG(3, 2), the projective space of dimension 3 over GF(2). It is one of the two nonisomorphic KTS having PG(3, 2) as its underlying STS. Altogether there are 4 resolvable STS(15)s but 7 nonisomorphic KTS(15), i..e. 7 nonisomorphic solutions to the Problem of 15 schoolgirls.

Clearly, for a KTS(v) to exist, the condition $v \equiv 3\ (mod\ 6)$ is necessary. It took more than 120 years before Ray-Chaudhuri and Wilson proved that this condition is also sufficient.

The following construction using PBDs is instrumental in the proof.

Theorem 8. *Let $(V,\mathcal{B})$ be a PBD(v,K), $K=\{k_1,\ldots,k_s\}$, $v\equiv 1$ $(mod\ 3)$, and suppose that for each $k_i\in K$, there exists a KTS$(2k_i+1)$. Then there exists a KTS$(2v+1)$.*

Proof. A KTS$(2v+1)$ will be constructed on the set $W=V\times\{1,2\}\cup\{\infty\}$ so that (w.l.o.g) $\{\infty,x_1,x_2\}$ is a block for all $x\in V$. Let $\mathcal{B}_x=\{B_{x1},\ldots,B_{xt}\}\subset\mathcal{B}$ be the blocks of the PBD(v,K) containing x. For each block $B\in\mathcal{B}_x$, put on the set $B\times\{1,2\}\cup\{\infty\}$ a KTS$(2|B|+1)$, $(U,\mathcal{B}_B,\mathcal{R}_B)$, making sure that $\{\infty,x_1,x_2\}$ is a block for all $x\in B$. Let R_{Bx} be the parallel class of $\mathcal{R}_B$ containing the triple $\{\infty,x_1,x_2\}$, and let $R_x=\cup_{B\in\mathcal{B}_x}R_{Bx}$ (the triple $\{\infty,x_1,x_2\}$ is taken just once). Then R_x is a parallel class on W, and $\mathcal{R}=\{R_x : x\in V\}$ is a resolution of a KTS$(2v+1)$. □

For all $v\equiv 1$ or 4 $(mod\ 12)$ there exists a PBD$(v,\{4\})$ (i.e. a Steiner system S$(2,4,v)$, see below), and for all $v\equiv 7$ or 10 $(mod\ 12)$, except for $v=10$ or 19, there exists a PBD$(v,\{4,7\}$(a result due to Brouwer). This, together with the above theorem, and with two individual examples of KTSs of orders 21 and 39 proves the existence of a KTS(v) for all $v\equiv 3$ $(mod\ 6)$,.

5. Subsystems and partial triple systems

An STS(w), say, $(W,\mathcal{C})$, is a *subsystem* of an STS(v), $(V,\mathcal{B})$, if $W\subseteq V$ and $\mathcal{C}\subseteq\mathcal{B}$. Then $(W,\mathcal{C})$ is said to be *embedded* in $(V,\mathcal{B})$ while $(V,\mathcal{B})$ is said to *contain* $(W,\mathcal{C})$. An embedding (or a subsystem) is *proper* if $|W|<|V|$. For a proper subsystem, one must have $|V|\geq 2|W|+1$. One may ask, conversely: given an STS(w), and an admissible integer v (that is, $v\equiv 1$ or 3 $(mod\ 6)$), $v\geq 2w+1$, can it be embedded into an STS(v)?

STSs have the so-called *replacement property*: Given an STS$(V,\mathcal{B}))$ with a sub-STS(w), $(W,\mathcal{C})$, and if $(W,\mathcal{D})$ is another STS(w) then $(V,(\mathcal{B}\backslash\mathcal{C})\cup\mathcal{D})$ is an STS(v). Actually, the replacement property holds much more generally, for any two *balanced* sets of triples T and T'; here, "balanced" means that a 2-subset P is contained in a triple of T if and only if it is contained in a triple of T'.

Doyen-Wilson Theorem. *Any STS(w) can be embedded into an STS(v) for any* $v \geq 2w+1$.

Apart from the original proof by Doyen and Wilson, a completely different proof is provided by Stern and Lenz, and yet another one in [3].

A *partial* triple system PTS(v) of order v is a pair $(V, \mathcal{B})$ where V is a v-set and $\mathcal{B}$ is a collection of 3-subsets of V called *blocks* or *triples* such that each 2-subset of V is contained in *at most* one triple of $\mathcal{B}$. The *leave* of a PTS $(V, \mathcal{B})$ is the graph $L = (V, E)$ where E contains as edges all those 2-subsets of elements of V that are *not* contained in the triples of $\mathcal{B}$.

Unlike for STSs, there is no restriction on the order of partial triple systems. A PTS $(V, \mathcal{B})$ is *completable* if there exists a set of further triples $\mathcal{C}$ such that $(V, \mathcal{B} \cup \mathcal{C})$ is an STS(v). The STS $(V, \mathcal{B} \cup \mathcal{C})$ is the *completion* of the PTS $(V, \mathcal{B})$. Clearly not every PTS(v) is completable. So, it is natural to ask whether any PTS can be *embedded* into an STS, i.e. given a PTS(v) $(V, \mathcal{B})$, does there exist an STS(w) $(W, \mathcal{C})$ such that $V \subseteq W$ and $\mathcal{B} \subseteq \mathcal{C}$? And if yes, what is the smallest w for which a PTS(v) can be embedded into an STS(w)?

This problem has only recently been solved by Bryant and Horsley [BH]: every PTS(v) can be embedded in an STS(w) where w is the smallest admissible integer (i.e. $w \equiv 1$ or 3 $(mod\ 6)$) such that $w \geq 2v+1$. The proof is quite involved. Here is a simple proof of a weaker result (which at the time was the strongest known result) due to Lindner [L] which shows that every PTS(v) can be embedded in an STS($6v+3$).

From a PTS(v), we first define a partial idempotent commutative quasigroup (V, o) by

(i) $x\ o\ x = x$ for all $x \in V$,

(ii) if $x \neq y$, $x\ o\ y = y\ o\ x = z$ if and only if $\{x, y, z\} \in \mathcal{B}$.

Note that either both $x\ o\ y$ and $y\ o\ x$ are defined, or neither is.

Next, we use Cruse's Theorem ("Every partial idempotent commutative quasigroup of order n can be embedded in an idempotent commutative quasigroup of order t for all odd $t \geq 2n+1$") to embed (V, o) in an idempotent commutative quasigroup (Q, o) of order $2v+1$. Put $W = Q \times \{1, 2, 3\}$, and use Bose's Construction to obtain from (Q, o) an STS($6v+3$), $(W, \mathcal{C})$. For each triple $T = \{x, y, z\} \in \mathcal{B}$, $\mathcal{C}$ contains the set $T(x, y, z)$ of 9 triples
$\{x_1, y_1, z_2\}, \{x_1, y_2, z_1\}, \{x_2, y_1, z_1\}, \{x_2, y_2, z_3\}, \{x_2, y_3, z_2\}, \{x_3, y_2, z_2\}$,
$\{x_3, y_3, z_1\}, \{x_3, y_1, z_3\}, \{x_1, y_3, z_3\}$;
replace $T(x, y, z)$ with another set $T'(x, y, z)$ of 9 triples

$\{x_1, y_1, z_1\}, \{x_2, y_2, z_2\}, \{x_3, y_3, z_3\}, \{x_1, y_2, z_3\}, \{x_1, y_3, z_2\}, \{x_2, y_1, z_3\}$,
$\{x_2, y_3, z_1\}, \{x_3, y_1, z_2\}, \{x_3, y_2, z_1\}$.

The sets $T(x, y, z)$ and $T'(x, y, z)$ are balanced, i.e. a 2-subset P is contained in a triple of T if and only if it is contained in a triple of T'. Moreover, if $\{x, y, z\}$ and $\{x', y', z'\}$ are two distinct triples in $\mathcal{B}$, no 2-subset of V can be contained in both $T(x, y, z)$ and $T(x', y', z')$. If $\mathcal{C}'$ is obtained from $\mathcal{C}$ by replacing for each $\{x, y, z\} \in \mathcal{B}$ the set $T(x, y, z)$ with $T'(x, y, z)$ then $(W, \mathcal{C}')$ is an STS$(6v + 3)$ which contains $(V, \mathcal{B})$ (in fact, three copies of $(V, \mathcal{B})$, one on each set $Q \times \{i\}$).

An *incomplete triple system* of order v with a hole of size w is a PTS(v), $(V, \mathcal{B})$, such that for some $W \subseteq V$ with $|W| = w$, each 2-subset $\{x, y\}$ of V with $x \in V \setminus W$, $y \in V$ is contained in exactly one triple of $\mathcal{B}$ while for $x, y \in W$, the 2-subset $\{x, y\}$ is not contained in any triple of $\mathcal{B}$. Such a partial triple system is denoted by ITS(v, w). If an ITS(v, w), $(V, \mathcal{B})$, exists with a hole on $W \subseteq V$ and also an STS(w), $(W, \mathcal{C})$ exists then $(V, \mathcal{B} \cup \mathcal{C})$ is an STS(v) (with $(W, \mathcal{C})$ as a subsystem).

An incomplete triple system TS(v, w) clearly exists if both $v, w \equiv 1$ or 3 $(mod\ 6)$ but may exist when neither of v, w satisfy this condition. Indeed, an ITS(v, w) exists whenever $v, w \equiv 5$ $(mod\ 6)$, and $v \geq 2w + 1$.

6. Colouring of Steiner triple systems

A (proper weak) *colouring* of an STS(v) $(V, \mathcal{B})$ is a mapping $\phi : V \to C$ (the set of colours) such that no triple is monochromatic. If $|C| = m$, we have an m-colouring. For each $c \in C$, the set $\phi^{-1} = \{x : \phi(x) = c\}$ is a *colour class*. The *chromatic number* $\chi(V, \mathcal{B})$ is the smallest m such that there exists an m-colouring of $(V, \mathcal{B})$.

There exists no nontrivial 2-chromatic STS. Bose's and Skolem's construction given above establish that fior all $v \equiv 1$ or 3 $(mod\ 6)$ there exists a 3-chromatic STS(v).

Exercise 9. Show that for $v \geq 7$ there is no 2-chromatic STS(v).

It is much more difficult to show the following.

Theorem 9. *A 4-chromatic STS(v) exists if and only if* $v \equiv 1$ *or* 3 $(mod\ 6)$ *and* $v \geq 21$.

Already in the 1960s, Erdös, Hajnal and Lovász showed that there exist *partial* triple systems with arbitrarily high chromatic number. If u_m is the smallest order of an m-chromatic partial triple system then

$$c_1 m^2 log\ m < u_m < c_2 m^2 log\ m$$

where c_1, c_2 are absolute constants. It follows that for any (partial) STS(v),

$$\chi \leq c\sqrt{v/log\ v}$$

where c is an absolute constant.

Theorem 10. *For all* $m \geq 3$ *there exists* v_m *such that for every* $v \geq v_m$, $v \equiv 1$ *or* 3 $(mod\ 6)$*, there exists an* m*-chromatic STS(v). Moreover, for smallest such* v_m*,*

$$C_1 m^2 log\ m < v_m < C_2 m^2 log\ m$$

.

However, the exact value of v_m is not known already for $m = 5$.

The spectrum $C(v)$ of chromatic numbers of STS(v) is the set $C(v) = \{m$: there exists an m-chromatic STS$(v)\}$. It was conjectured, but remains unproved, that $C(v)$ is always an interval.

An m-chromatic STS(v) is *uniquely colourable* if any m-colouring of the STS produces the same partition of the element set into colour classes. A colouring of an STS is *equitable* if the cardinalities of the colour classes differ by at most one. A colouring is a *bicolouring* if there are no triples coloured with three distinct colours.

Consider now colouring the triples of an STS. A *block-colouring* of an STS(v), $(V, \mathcal{B})$, is a mapping $\psi : \mathcal{B} \to C$ (the set of (colours) such that if $\psi(B) = \psi(B')$ for $B, B' \in \mathcal{B}$, $B \neq B'$ then $B \cap B' = \emptyset$. If $|C| = q$ then ψ is a q-colouring. For each $c \in C$, $\psi^{-1}(c)$ is a *block-colour class.* The *chromatic index* $\chi'(V, \mathcal{B})$ of $(V, \mathcal{B})$ is the smallest q for which $(V, \mathcal{B})$ has a q-block-colouring. Every block-colour class is a *partial parallel class*, thus $\chi'(V, \mathcal{B}) \geq |\mathcal{B}|/\lfloor \frac{v}{3} \rfloor$ so $\chi' \geq \frac{v-1}{2}$ when $v \equiv 3$ $(mod\ 6)$ and $\chi' \geq \frac{v+1}{2}$ when $v \equiv 1$ $(mod\ 6)$. The existence result for KTSs can be restated as:

For every $v \equiv 3$ (mod 6) there exists an STS(v) with (minimum possible) chromatic index $\frac{v-1}{2}$.

For $v \equiv 1$ (mod 6), a *Hanani triple system* is an STS(v) whose blocks can be partitioned into $\frac{v-1}{2}$ almost parallel clases, and a single partial parallel class with $\frac{v-1}{6}$ blocks. A Hanani triple system of order v exists if and only if $v \equiv 1$ (mod 6), $v \notin \{7, 13\}$. It follows that for every $v \equiv 1$ (mod 6), $v \geq 19$, there exists an STS(v) with (minimum possible) chromatic index $\frac{v+1}{2}$.

The chromatic index for the unique STS(7) is 7, the chromatic index of the two nonisomorphic STS(13) is 8. For $v > 7$, not a single STS(v) is known for which the chromatic index would exceed the minimum possible by more than 2. The following is an open problem.

Conjecture. For $v > 7$ and any STS(v), the chromatic index $\chi' \in \{min_v, min_v + 1, min_v + 2\}$ where $min_v = \frac{v-1}{2}$ for $v \equiv 3$ (mod 6), and $min_v = \frac{v+1}{2}$ for $v \equiv 1$ (mod 6).

Infinite classes of STSs for which $\chi' = min_v + 2$ are known. One of these is the class of projective triple systems of even dimension, i.e. PG($2m, 2$) which are STS($2^{2m+1} - 1$), $m \geq 2$. An argument by R. Wilson shows that such projective triple systems cannot contain an almost parallel class, therefore for them $\chi' \geq min_v + 2$. A recent result by M. Meszka establishes equality.

* * *

Further topics on Steiner triple systems include (not exhaustively) enumeration, automorphisms, independent sets, leaves, coverings, neighbourhoods, configurations, intersections, large sets, orthogonal resolutions etc. etc. (cf. [1], [2], [3], [4]).

III. STEINER SYSTEMS S($2, 4, v$)

A Steiner system S($2, 4, v$) is a pair ($V, \mathcal{B}$) where V is a v-set and $\mathcal{B}$ is a collection of 4-subsets of V called blocks (or sometimes quadruples) such that each 2-subset of V is contained in exactly one block. Hanani [H] proved that a Steiner system S($2, 4, v$) exists if and only if $v \equiv 1$ or 4 (mod 12). The smallest nontrivial system is S($2, 4, 13$), the projective plane of order 3, PG($2, 3$), where $V = Z_{13}$, and $\mathcal{B} = \{\{i, i+1, i+3, i+9\} : i \in Z_{13}\}$. It is unique up to an isomorphism, and its full automorphism group is 2-transitive of order 5616. The Steiner system S($2, 4, 16$) is also unique; it is the affine plane of order 4, Its full automorphism group is also 2-transitive and has order 16.15.12.2. The number of nonisomorphic S($2, 4, 25$) is 18 but the exact number of nonisomorphic S$(2,4,28)$ (the next order) is not known, only that there are 4466 nonisomorphic S$(2,4,28)$ with nontrivail automorphism group.

The complexity of the isomorphism problem for S$(2,4,v)$s is not known. Just as for STSs, the isomorphism of S$(2,4,v)$s can be tested in subxeponential time.

Hanani's existence proof is recursive. Starting with a direct construction of S$(2,4,v)$ for orders $13,16,25,28,37$, one then uses a PBD(u,K) where $K=\{4,5,8,9,12\}$; such a PBD exists for all $u\equiv 0,1$ $(mod\ 4)$ [2]. If $(X,\mathcal{B})$ is such a PBD, define $V=X\times\{1,2,3\}\cup\{\infty\}$. For each block $B\in\mathcal{B}$, construct an S$(2,4,|B|+1)$ on the set $B\times\{1,2,3\}\cup\{\infty\}$ so that for each $x\in X$, $\{\infty,x_1,x_2,x_3\}$ is always a block. The result is an S$(2,4,3v+1)$.

Unlike for STSs, a simple direct proof of the existence of S$(2,4,v)$s is so far absent.

Concerning cyclic S$(2,4,v)$s, here much less is known than for cyclic STSs. In a cyclic S$(2,4,v)$ with $v\equiv 1$ $(mod\ 12)$, there are $\frac{v-1}{12}$ full orbits of blocks (those of length v) and no short orbit, while if $v\equiv 4$ $(mod\ 12)$, there are $\frac{v-4}{12}$ full orbits and one short orbit (of length $\frac{v}{4}$).

There exists no cyclic S$(2,4,16)$ or S$(2,4,25)$ but there exist systems with automorphism group acting transitively on the set of elements. This is clear for he unique S$(2,4,16)$ which is AG$(2,4)$, the (unique) affine plane of order 4. An S$(2,4,25)$ with automorphism group $Z_5\times Z_5$ has as blocks $\{0_0,1_0,0_1,2_2\}$, $\{0_0,2_0,0_2,4_4\}$ $mod(5,5)$; the order of the full automorphism of this S$(2,4,25)$ is 150.

In his 1939 paper, Bose gave the following construction which for *p prime* yields a cyclic S$(2,4,v)$.

Theorem 11. *Let $v=p^n=12t+1$, and let α be a primitive element of GF(p^n) such that $\alpha^{4t}-1=\alpha^q$ for some odd q. Then the blocks $\{0,\alpha^{2i},\alpha^{4t+2i},\alpha^{8t+2i}\}$, $i=0,1,\dots,t-1$ are the base blocks for an S($2,4,v$).*

The smallest orders for which this theorem yields cyclic S$(2,4,v)$s are $v=13,37,61,73,97,\dots$. It is known that cyclic S$(2,4,v)$s exist for all $v\equiv 1,4$ $(mod\ 12)$, $v\leq 613$ except for $v=16,25,28$ for which they do not exist. The conjecture that for all admissible $v\geq 37$ there exits cyclic S$(2,4,v)$s remains open.

Just as there is a relationship between STSs and Steiner quasigroups, tehre exists a relationship of Steiner systems S$(2,4,v)$ to another class of algebras, namely *Stein quasigroups.* In the literature, there are two kinds of Stein quasigroups. A quasigroup (V, o) satisfying the *Stein's law*, sometimes called *first Stein's law* or *law of semisymmetry*,

$$x\ o\ (x\ o\ y) = y\ o\ x \qquad (1)$$

is a Stein's quasigroup of the first kind, or S-quasigroup for short. S-quasigroups are idempotent, anticommutative (i.e, $x\ o\ y \neq y\ o\ x$ for $x \neq y$), and nonassociative.

An example of an S-quasigroup of order 4 is

o	1	2	3	4
1	1	3	2	4
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4.

The second kind of Stein quasigroups are those satisfying the laws

$x\ o\ x = x$

$(x\ o\ y)\ o\ y = y\ o\ x$

$(y\ o\ x)\ o\ y = x.$

The third of these laws is sometimes called the *law of left semisymmetry..*

Call quasigroups satisfying these laws S^*-quasigroups. While an S^*-quasigroup is an S-quasigroup, the converse need not hold. However, the S-quasigroup of order 4 given above is also an S^*-quasigroup.

Let (V, o) be an S^*-quasigroup of order v. Define

$\mathcal{B} = \{x, y, x\ o\ y, y\ o\ x\} : x, y \in V, x \neq y\}.$

Then $(V, \mathcal{B})$ is an $\mathrm{S}(2,4,v)$. Conversely, given an $\mathrm{S}(2,4,v)$, $(V, \mathcal{B})$, obtain from it an S^*-quasigroup as follows. For every block $B \in \mathcal{B}$, choose arbitrarily a bijection $\phi_B : B \rightarrow \{1, 2, 3, 4\}$. On V, define a binary operation "$*$" by

$x\ *\ x = x\ o\ x\ (= x)$

$x\ *\ y = \phi_B^{-1}(\phi_B(x)\ o\ \phi_B(y))$ for $x \neq y, x, y \in B$

where "o" is a binary operation on $\{1, 2, 3, 4\}$ as defined above. Then $(V, *)$ is an S^*-quasigroup.

Concerning embeddings of $\mathrm{S}(2,4,v)$s, a theorem analogous to the Doyen-Wilson Theorem but having a much more complicated proof is due to Rees and Stinson.

Rees-Stinson Theorem. *Any S(*$2,4,w$*) can be embedded in an S(*$2,4,v$*) for any* $v \geq 3w+1$*.*

A more general version of the Rees-Stinson Theorem is the following.

Theorem 12. *A Steiner system S(*$2,4,w$*) with a hole of size* v*,* $v < w$*, exists if and only if* $w \geq 3v+1$*, and*

(i) $v, w \equiv 1$ *or* 4 $(mod\ 12)$*, or*

(ii) $v, w \equiv 7$ *or* 10 $(mod\ 12)$*.*

Ganter proved in 1971 that every *partial* S$(2,4,w)$ ca be embedded in some S$(2,4,v)$. However, the embedding provided, while finite, is at worst exponential in the size of the partial triple system. To find a polynomial size embedding for partial S$(2,4,v)$s is an open problem.

A *colouring* of an S$(2,4,v)$, $(V,\mathcal{B})$, is a mapping $\phi : V \to C$ (the set of colours) such that for all $B \in \mathcal{B}$, $|\phi(B)| > 1$ where $\phi(B) = \cup_{x \in B}\phi(x)$. For each $c \in C$, the set $\phi^{-1}(c) = \{x : \phi(x) = c\}$ is a *colour class.* If $|C| = m$, we have an m-colouring. The *chromatic number* $\chi = \chi(V,\mathcal{B})$ is the smallest m for which there exists an m-colouring of $(V,\mathcal{B})$. If $\chi(V,\mathcal{B}) = m$, the system is m-chromatic.

Unlike STSs whose chromatic number must be at least 3 if $v > 3$, Steiner systems S$(2,4,v)$ may be 2-chromatic. Each of the unique S$(2,4,v)$s for $v = 4, 13, 16$ is 2-chromatic, and of the 18 S$(2,4,25)$s, two are 2-chromatic. The following holds.

Theorem 13. *A* 2*-chromatic S(*$2,4,v$*) exists for all admissible orders* $v \equiv 1, 4$ $(mod\ 12)$*.*

The following was proved in [RWCZ].

Theorem 14. *A* 3*-chromatic S(*$2,4,v$*) exists if and only if*
$v \equiv 1$ *or* 4 $(mod\ 12)$ *and* $v \geq 25$*.*

There exist S$(2,4,v)$s with an arbitrarily high chromatic number. Moreover:

Theorem 15. *For every $m \geq 2$, there exists v_m such that for all admissible orders $v \geq v_m$, there exists an m-chromatic S(2, 4, v).*

The complexity of computing the chromatic number of $\mathrm{S}(2,4,v)$s is unknown.

An $\mathrm{S}(2,4,v)$ $(V,\mathcal{B})$ can be *extended* if there exists an $\mathrm{S}(3,5,v+1)$ $(V \cup \{\infty\}, \mathcal{C})$ such that $(V,\mathcal{B})$ is a derived design of $(V \cup \{\infty\}, \mathcal{C})$ through the element ∞ (i.e. the blocks of $\mathcal{B}$ are obtained by taking all blocks of $\mathcal{C}$ containing ∞ and deleting ∞ from them). An affine space $\mathrm{AG}(n,q)$ can be extended to an inversive space $\mathrm{S}(3,q+1,q^n+1)$, so for each positive n, there exists an $\mathrm{S}(2,4,4^n)$ which can be extended to an $\mathrm{S}(3,5,4^n+1)$. A necessary condition for the existence of an $\mathrm{S}(2,4,v)$ extendable to $\mathrm{S}(3,5,v)$ is $v \equiv 1, 4, 16, 25, 40$ or 49 $(mod\ 60)$.

Exercise 10. Show that the necessary conditions for the existence of an $\mathrm{S}(3,5,v)$ is $v \equiv 2, 5, 17, 26, 41, 50$ $(mod\ 60)$.

A Steiner system $\mathrm{S}(2,4,v)$ $(V,\mathcal{B})$ is *resolvable* if $\mathcal{B}$ can be partitioned into $\frac{v-1}{3}$ parallel classes.

Theorem 16. *A resolvable S(2, 4, v) exists if and only if $v \equiv 4$ (mod 12)*

A *block–colouring* of an $\mathrm{S}(2,4,v)$, $(V,\mathcal{B})$ is a mapping $\psi : \mathcal{B} \to C$ (the set of colours) such that if $\psi(B) = \psi(B')$ for $B, B' \in \mathcal{B}$, $B \neq B'$ then $B \cap B' = \emptyset$. If $|C| = k$ then ψ is a k-block-colouring. For $c \in C$, $\psi^{-1}(c)$ is a block-colour class. The chromatic index $\chi'(V,\mathcal{B})$ of $(V,\mathcal{B})$ is the smallest k for which $(V,\mathcal{B})$ has a k-block-colouring. Since $\chi'(V,\mathcal{B}) \geq |\mathcal{B}|/\frac{v}{[4]}$, always $\chi' \geq \frac{v-1}{3}$. The existence of resolvable $\mathrm{S}(2,4,v)$s means that for every $v \equiv 4$ $(mod\ 12)$ there exists a Steiner system $\mathrm{S}(2,4,v)$ with chromatic index $\frac{v-1}{3}$ (the minimum possible).

When $v \equiv 1$ $(mod\ 12)$, $\chi' \geq \frac{v+2}{3}$. For $v \leq 25$, there is no $\mathrm{S}(2,4,v)$ with chromatic index equal to the minimum possible value $\frac{v+2}{3}$., It is an open question whether such systems exist for $v \geq 37$.

As for upper bounds, $\chi' \leq \frac{4v-1}{3}$ for any $\mathrm{S}(2,4,v)$, and $\chi' \leq v$ for cyclic $\mathrm{S}(2,4,v)$s.

The complexity of computing the chromatic index of $\mathrm{S}(2,4,v)$s is unknown.

A recent survey of results and problems on $\mathrm{S}(2,4,v)$s is [RR] which treats many other properties and problems on $\mathrm{S}(2,4,v)$s.

IV. STEINER QUADRUPLE SYSTEMS

Steiner systems $\mathrm{S}(3,4,v)$ are called *Steiner quadruple systems* (SQS). An $\mathrm{SQS}(v)$ is a pair $(V,\mathcal{B})$ where V is a finite set of elements, and $\mathcal{B}$ is a collection of 4-subsets of V called *quadruples* such that every 3-subset of V is contained in exactly one quadruple. One has $|\mathcal{B}| = \frac{v(v-1)(v-2)}{24}$.

If $x \in V$, let $\mathcal{B}(x) = \{B' = B \setminus \{x\} : x \in B\}$. Then $(V \setminus \{x\}, \mathcal{B}(x))$ is an $\mathrm{STS}(v-1)$. It follows that $v \equiv 2$ or 4 $(mod\ 6)$ is a necessary condition for the existence of an $\mathrm{SQS}(v)$. The triple system so formed is the *derived* STS of the SQS. An old conjecture that every STS is a derived STS of some SQS remains unproved.

Example 8. An SQS(8): $V = Z_7 \cup \{\infty\}$,
$\mathcal{B} = \{\infty, i, i+1, i+3\}, \{i, i+2, i+3, i+4\} : i \in Z_7\}$

Example 9. An SQS(10): $V = Z_{10}$, $\mathcal{B} = \{\{i, i+1, i+3, i+4\},$
$\{i, i+1, i+2, i+6\}, \{i, i+2, i+4, i+7\} : i \in Z_{10}\}$.

A *Boolean* SQS has as its set of elements $V = Z_2^n$ and as its blocks the quadruples (x,y,z,w) of distinct binary words of length n such that $x+y+z+w = \bar{0}$.

Hanani was first to prove that $v \equiv 2$ or 4 $(mod\ 6)$ is also sufficient for the existence of $\mathrm{SQS}(v)$. His recursive proof was quite complicated but has since been simplified by Hartman, Lenz and others. No direct proof is known to-date.

The simplest recursive construction is "duplication".

Theorem 17. *If there exists an SQS(v) then there exists an SQS($2v$).*

Proof. Let $(V,\mathcal{B})$ and $(W,\mathcal{C})$ be two $\mathrm{SQS}(v)$, $V \cap W = \emptyset$. Let $\mathcal{F} = \{F_1, \ldots, F_{v-1}\}$ and $\mathcal{G} = \{G_1, \ldots, G_{v-1}\}$ be any two 1-factorizations of K_v on V and W, respectively, let α be any permutation of degree v on W. Let $V \cup W$, form the set of quadruples $\mathcal{E} = \{\{x_1, y_1, z_2, w_2\} : \{x,y\} \in F_i, \{z,w\} \in \alpha G_i, F_i \in \mathcal{F}, G_i \in \mathcal{G}\}$. Then $(W, (\mathcal{B} \times \{1\}) \cup (\mathcal{C} \times \{2\}) \cup \mathcal{E})$ is an $\mathrm{SQS}(2v)$.

Note that two copies of the original $\mathrm{SQS}(v)$ are embedded in the resulting $\mathrm{SQS}(2v)$. There need be no relationship between the two $\mathrm{SQS}(v)$ or between the two 1-factorizations.

The above construction si actually a special case of a "generalized product onstruction". But the simpler fact that the existence of an $\mathrm{SQS}(v)$ and an SQS(w) implies the existence of an SQS($v.w$) follows easily from the equivalence of SQSs with a certain class of ternary algebras.

Given an SQS(v), $(V, \mathcal{B})$, we may define a ternary operation $< \, , \, , \, >$ on V by

(1) $< x, x, y >= y$,

(2) $< x, y, z >= u$ whenever $\{x, y, z, u\} \in \mathcal{B}$.

The resulting algebra is a ternary quasigroup called *Steiner* 3-*quasigroup*. It satisfies the identities

(i) $< x, x, y >= y$ (the generalized idempotent law),

(ii) $< x, y, z >=< x, z, y >=< y, x, z >$,

(iii) $< x, y, < x, y, z >>= z$.

Conversely, from every 3-quasigroup $(V, <, , >)$ satisfying (i), (ii), and (iii) we can obtain an SQS: just define $\mathcal{B} = \{\{x, y, z, < x, y, z >\} :$
$x, y, z \in V$ distinct$\}$

So, Steiner 3-quasigroups form an equational class of algebras. Steiner 3-quasigroups that satisfy also the identity

(iv) $<< x, w, y >, w, z >=< x, w, < y, w, z >>$

also form an equational class of algebras. The corresponding SQSs are precisely the Boolean SQS.

Returning to the existence proof for SQSs, one needs several further recursive rules in addition to the doubling rule. One of these is the following.

Theorem 18. *If there exists an SQS(v) then there exists an SQS($3v-2$).*

Proof. Let $(V, \mathcal{B})$ be an SQS(v), and let $(V_a, \mathcal{B}_a)$ be its derived STS($v-1$) through the element a, and let $Q = \{B \in \mathcal{B} : a \notin B\}$. We construct an SQS($3v-2$), $(W, \mathcal{C})$, where $W = (V_a \times Z_3 \cup \{\infty\}$. Let $\mathcal{C}$ be a collection of 4-subsets of W contaning the following three types of 4-subsets.

(1) the 4-subsets $\{\infty, x_0, x_1, x_2\}$ for all $x \in V_a$,

(2) if $B = \{a, x, y, z\} \in \mathcal{B}$, all quadruples of an SQS(10), $(T, \mathcal{B}_B)$, where $T = \{\infty\} \cup \{x, y, z\} \times Z_3$ and $\mathcal{B}_B$ includes the four quadruples $\{\infty, x_1, x_2, x_3\}, \{\infty, y_1, y_2, y_3\}, \{\infty, z_1, z_2, z_3\}$ and $\{\infty, x_3, y_3, z_3\}$.

(3) if $\{x, y, z, w\} \in \mathcal{B}$ and $a \notin B$, the 4-subsets $\{x_i, y_j, z_k, w_l\}$ for all i, j, k, l such that $i + j + k + l \equiv 0$ (mod 3).

V. SOME OTHER TYPES OF COMBINATORIAL DESIGNS

1. Cycle decompositions

A *k-cycle system* of order v ($k\mathrm{CS}(v)$) is a pair $(V, \mathcal{C})$ where $\mathcal{C}$ is a collection of edge-disjoint k-cycles of the complete graph K_v with vertex set V. A $3\mathrm{CS}(v)$ is the same as an $\mathrm{STS}(v)$. An obvious necessary consdition for the existence of a $k\mathrm{CS}$ is that v must be odd, $v \geq k$, and $k | \binom{v}{2}$. The sufficiency of this condition has been proved in [AG], [Saj].

So, for example, a 4CS(v) exists if and only if $v \equiv 1$ $(mod\ 8)$. An example of a 4CS(9) is given by $V = Z_9$, $\mathcal{C} = \{(i, i+1, i+5, i+2) : i \in Z_9\}$.

Let $v = 8n+1, n \geq 2$. Let X be a set, $|X| = 4n$, and let $H = \{h_1, h_2, \ldots, h_n\}$ be a partition of X into 4-subsets ("holes"). Let $V = (X \times \{1,2\}) \cup \{\infty\}$. For each hole h_i, $i = 1‘, 2, \ldots, n$, put on $(h_i \times \{1,2\}) \cup \{\infty\}$ a copy of the 4CS(9) from the example above. For two distinct elements x, y from different holes of H, form the 4-cycle (x_1, y_1, x_2, y_2). If one collects all these 4-cycles into $\mathcal{C}$ then $(V, \mathcal{C})$ is a $4\mathrm{CS}(v)$.

Similarly, a $5\mathrm{CS}(v)$, also called a *pentagon system*, exists if and only if $v \equiv 1$ or 5 $(mod\ 10)$. To see this, consider the folllowing two constructions.

1. Let $v \equiv 5$ $(mod\ 10)$, $v = 10n+5$. Let (Q, o) be an idempotent commutative quasigroup of order $2n+1$, and let $V = Q \times Z_5$. For each $x \in Q$, form two pentagons $(x_1, x_2, x_3, x_4, x_5)$ and $(x_1, x_3, x_5, x_2, x_4)$ (i.e. a 5CS(5)). For distinct $x, y \in Q$, form the pentagons $(x_i, y_i, x_{i+1}, (x\ o\ y)_{i+3}, y_{i+1})$, $i \in Z_5$. The collection of all these pentagons forms a $5\mathrm{CS}(v)$.

2. Let $v \equiv 1$ $(mod\ 10)$, $v = 10n+1$. Let (Q, o), $Q = \{1, 2, \ldots, 2n\}$, be a commutative quasigroup with holes $H = \{\{1,2\}, \{3,4\}, \ldots, \{2n+1, 2n\}\}$. It is not difficult to see that such a quasigroup exists for all even orders ≥ 6. Let $V = (Q \times Z_5) \cup \{\infty\}$. For each hole $h \in H$, put a copy of a 5CS(11) on $(h \times Z_5) \cup \{\infty\}$. An example of a 5CS(11) is given by $(V, \mathcal{C})$ where $V = Z_{11}$, $\mathcal{C} = \{(i, i+2, i+8, i+4, i+3) : i \in Z_{11}\}$, or (another example) $\mathcal{C} = \{(i, i+2, i+9, i+4, i+1) : i \in Z_{11}\}$.

For distinct $x, y \in Q$ and from different holes of H, form the pentagons $(x_i, y_i, x_{i+1}, (x\ o\ y)_{i+3}, y_{i+1})$. The collection of all these pentagons is a $5\mathrm{CS}(v)$.

This proves the existence of a $5\mathrm{CS}(v)$ for all $v \equiv 1$ or 5 $(mod\ 10)$ except when $v = 21$. For $v = 21$, take a $\mathrm{BIBD}(21, 5, 1)$ (i.e. the projective plane $\mathrm{PG}(2, 4)$) and put a copy of a 5CS(5) on each block.

A kCS(v), $(V, \mathcal{C})$, is 2-*perfect* if any two distinct vertices of V are joined by a path of length 2 in exactly one k-cycle of $\mathcal{C}$. Of the two examples of a 5CS(11) above, the first is 2-perfect while the second is not.

If $(V, \mathcal{C})$ is a kCS(v) $k \geq 3$, one can define a binary operation "o" on V as follows:

(1) $x \ o \ x = x$ for all $x \in V$;

(2) for $x \neq y, \ \ x \ o \ y = z$ and $y \ o \ x = w$ if $(\dots, w, x, y, x, \dots) \in \mathcal{C}$.

This is sometimes called the Standard Construction. The resulting groupoid (V, o) may or may not be a quasigroup.

Theorem 19. *The groupoid (V, o) obtained by the Standard Construction from a kCS(v) $(V, \mathcal{C})$ is a quasigroup if and only if $(V, \mathcal{C})$ is 2-perfect.*

The class of Steiner quasigroups can be equationally defined. Similarly, the class of quasigroups from 2-perfect pentagon systems can be equationally defined. The set of identities for quasigroups coresponding to *Steiner pentagon systems* is

(i) $x \ o \ x = x$,

(ii) $(y \ o \ x) \ o \ x = y$,

(iii) $x \ o \ (y \ o \ x) = y \ o \ (x \ o \ y)$.

A 4CS is never 2-perfect so the groupoid obtained by the Standard Construction from a 4CS is never a quasigroup.

By contrast, 2-perfect 6-cycle systems do exist. Moreover, they exist for all orders $v \equiv 1$ or 9 $(mod\ 12)$ (just as do 6CSc without the additional condition of 2-perfectness) except that there exists no 2-perfect 6CS(9). But 2-perfect 6CSs *cannot* be equationally defined.

A 7CS(v) exists if and only if $v \equiv 1$ or 7 $(mod\ 14)$. For each such order, there also exists a 2-perfect 7CS. The class of of 2-perfect 7CSs can be equationally defined. A defining set of identities for 2-perfect 7-cycle systems is

(i) $x \ o \ x = x$,

(ii) $(y \ o \ x) \ o \ x = y$,

(iii) $(x \ o \ y)(y \ o \ (x \ o \ y)) = (y \ o \ x)(x \ o \ (y \ o \ x))$.

It was shown by Bryant and Lindner [BL] that 2-perfect k-cycle systems can be equationally defined only for $k = 3, 5$ and 7.

Another way to define a binary operation, given a kCS $(V, \mathcal{C})$ when k is odd is as follows. In a k-cycle where k is odd, the stabilizer of any edge has exactly one fixed point (graphs having this property are called focal; there are many graphs other than odd cycles which are focal, e.g. $K_{2,3}$). One can define on V a binary operation "o" by

(i) $x \ o \ x = x$;

(ii) fior $x \neq y$, $x \ o \ y = z$ where z is the (unique) fixed point of the stabilizer of the edge $\{x, y\}$.

The resulting groupoid is always commutative. For odd $k = 2m+1$, the groupoid (V, o) obtained in this way from a $(2m+1)$CS $(V, \mathcal{C})$ is a quasigroup if and only if $(V, \mathcal{C})$ is m-perfect, that is, every pair of vertices $x \neq y$ are joined by a path of length m in exactly one k-cycle.

2. Graph decompositions

A decomposition of the complete multigraph λK_v into edge-disjoint copies of a graph G is sometimes called a *G-design* of order v and index λ. Such G-designs have been considered for many classes of graphs G, such as paths, trees, stars, cycles (see previous section), cubes, graphs with small number of vertices etc. The main question asked is that of the existence of G-designs. A good survey on G-designs can be found in [2].

3. One-factorizations, Room squares and Howell designs

One-factorizations of the complete graph K_n were already mentioned briefly. For a graph G to have a 1-factorization, it clearly must be regular of Class 1. The literature on 1-factorizations is quite extensive and includes at least one book and several survey articles. The best known 1-factorization of K_n often denoted as GK_{2n} is $(V, \mathcal{F})$ where $V = Z_{2n-1} \cup \{\infty\}$, and $\mathcal{F} = \{F_1, \ldots, F_{2n-1})$, $F_i = \{\{i+j, i-j\} : j = 1, 2, \ldots, n-1\} \cup \{\{i, \infty\}$, $i = 0, 1, \ldots, 2n-2$. The automorphism group of GK_{2n} has order $(2n-1).\phi(2n-1)$. It fixes one element, and when $2n-1$ is a prime, it is 2-transitive on the remaining elements.

Generally, 1-factorizations with automorphism group fixing one element and transitive on the remaining elements form a large class containing many interesting members. Because of the existence of an automorphism fixing one element and permuting the rest in a single cycle of length $2n-1$, the 1-factorizations of this class are called 1–rotational (or sometimes starter-generated).

Somewhat related to the series of 1-factorizations GK_{2n} is the series of 1-factorizations AK_{2n} (n odd). Let $V = Z_n \times \{1, 2\}$, and $\mathcal{F} = \{F_i : i = 1, 2, \ldots, n\} \cup \{G_i : i = 1, 2, \ldots, n-1\}$ where $F_i = \{\{i_1, i_2\}\} \cup \{\{(i+j)_k, (i-j)_k\} : i \in Z_n,\ j = 1, 2, \ldots, \frac{n-1}{2},\ k = 1, 2\}$, $G_i = \{\{j_1, (j+i)_2\} : j \in Z_n\}$.

One could also require that the automorphism group act transitively on the set of elements (i.e. vertices of the complete graph), in particular, be a cyclic group acting on the $2n$ vertices. This simple requirement for *cyclic* 1-factorizations, so natural and efficient when considering block designs, is less natural here, since it necessarily implies that under the action of cyclic group the 1-factors fall in several orbits, of varying lengths. Nevertheless, it has been shown that a cyclic 1-factorization of K_{2n} exists if and only if the order $2n$ is *not* a power of 2 greater than 4. When n is a prime, GA_{2n} is cyclic.

Given a 1-factorization of K_{2n}, $\mathcal{F} = \{F_1, \ldots, F_{2n-1}\}$, the union of any two distinct 1-factors $F_i \cup F_j$ is a 2-regular graph whose all cycles are of an even length. When for any $F_i, F_j \in \mathcal{F}$, the union $F_i \cup F_j$ is a hamiltonian cycle, the 1-factorizations is *perfect.* The 1-factorization GK_{2n} is perfect whenever $2n-1$ is a prime, and GA_{2n} is perfect wheneveer n is a prime. This was first shown by Kotzig in his 1963 Smolenice paper where he also conjectured that a perfect 1-factorization of K_{2n} exists for all $n \geq 2$. This conjecture is still open, as the existence of a perfect 1-factorization has been proved only for a handful of other values of n. Currently the smallest complete graph for which the existence of a perfect 1-factorization remains in doubt is K_{56}.

Two 1-factorizations of K_{2n}, $\mathcal{F} = \{F_1, \ldots, F_{2n-1}\}$, $\mathcal{G} = \{G_1, \ldots, G_{2n-1}\}$, are *orthogonal* if $|F_i \cap G_j| \leq 1$ for all $i, j \in \{1, 2, \ldots, 2n-1\}$.

* * *

Let N be an n-set. A *Room square* R of order n based on N is an $(n-1) \times (n-1)$ square array with the folowing properties:

(1) Every cell of R is either empty or contains a 2-subset of N;

(2) Every element of N is contained in exactly one cell of each row and of each column;

(3) Every 2-subset of N is contained in exactly one cell of R.

Each row (column) of R contains $\frac{n}{2} - 1$ empty cells and $\frac{n}{2}$ nonempty cells. The order n must be even.

An example of a Room square of order 8 is

01	37	56	–	24	–	–
–	02	14	67	–	35	–
–	–	03	25	17	-	46
57	–	–	04	36	12	–
–	16	–	–	05	47	23
34	–	27	–	–	06	15
26	45	–	13	–	–	07

The pairs of elements in the nonempty cels of each row (each column) are 1-factors, and the collection of 1-factors from all rows (all columns) forms a 1-factorization, and the two 1-factorizations are orthogonal. Thus a Room square of order n exists if and only if there exists a pair of orthogonal 1-factorizations of K_{2n}.

Two Steiner triple systems $(V, \mathcal{B}_1)$, $(V, \mathcal{B}_2)$ are *orthogonal* if

(1) $\mathcal{B}_1 \cup \mathcal{B}_2 = \emptyset$, i.e. they are disjoint, and

(2) if $\{a, b, x\}, \{c, d, x\} \in \mathcal{B}_1, \{a, b, y\}, \{c, d, z\} \in \mathcal{B}_2$ then $y \neq z$.

Theorem 20. *If there exists a pair of orthogonal STS(v) then there exists a Room square of order $v+1$.*

Proof. The two 1-factorizations obtained from the two STSs are orthogonal.

However, the converse does not hold.

Let G be an additive abelian group of odd order $2n-1$. A *starter* in G is a partition X of $G \setminus \{0\}$ into 2-subsets,

$X = \{\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_{n-1}, y_{n-1}\}$ such that

(i) $\{x_1, x_2, \ldots, x_{n-1}, y_1, y_2, \ldots, y_{n-1}\} = G \setminus \{0\}$,

(ii) $\{\pm(x_1 - y_1), \pm(x_2 - y_2), \ldots, \pm(x_{n-1} - y_{n-1})\} = G \setminus \{0\}$.

Two special types of starters are

(1) *patterned starter*:

$x_i + y_i = 0$ for all $i = 1, 2, \ldots, n-1$, i.e. $y_i = -x_i$.

(2) *strong starter*:

$x_i + y_i \neq 0, \quad x_i + y_i \neq x_j + y_j$ for $i \neq j$,

i.e. all sums $x_i + y_i$ are distinct and nonzero.

An *adder* A_X for a starter X is an ordered set of $n-1$ distinct elements of G, $A_X = (a_1, a_2, \ldots, a_{n-1})$, such that

$\{x_1 + a_1, x_2 + a_2, \ldots, x_{n-1} + a_{n-1}, y_1 + a_1, y_2 + a_2, \ldots, y_{n-1} + a_{n-1}\} = G \setminus \{0\}$.

Theorem 21. *If there exists in an abelian group G of order $2n-1$ with a starter and an adder then there exists a Room square of order $2n = |G|+1$.*

Proof. Let the elements of G be $0 = g_1, g_2, \dots, g_{2n-1}$. Let the starter be $X = \{\{x_i, y_i\} : i = 1, 2, \dots, n-1\}$, and adder be $A_X = (a_1, a_2, \dots, a_{n-1})$. The elements of a Room square R will be $\{\infty\} \cup G$. Form the first row of R as follows: place the 2-subset $\{\infty, g_1\}$ in the cell (g_1, g_1). For $k \neq 1$, place $\{x_i, y_i\}$ in the cell (g_1, g_k) if $-g_k = a_i$; otherwise, lave the cell (g_1, g_k) empty. Develop then the othwer rows cyclically, i.e. for $j > 1$ place $\{x_i + g_j, y_i + g_j\}$ in the cell (g_j, g_k) provided $\{x_i, y_i\}$ is in the cell $(g_1, g_k - g_j)$. Otherwise, i.e. when the cell $(g_1, g_k - g_j)$ is empty, leave (g_j, g_k) also empty. If one defines $\infty + j = \infty$ for all $g \in G$ then this works also for the diagonal cells. One needs to verify that R is a Room square of order $2n$ based on $\{\infty\} \cup G$. There are $\binom{2n}{2}$ nonempty cells; these are all pairs $\{x_i + g, y_i + g\}$ where $g \in G$ and $i = 1, 2, \dots, n-1$, plus the diagonal entries $\{\infty, g_i\}$. If $\{g_a, g_b\}$ is a 2-subset of G then, by the properties of a starter, there exists a pair (x_i, y_i) such that $\pm(x_i - y_i) = g_a - g_b$. If we write $g = g_b - y_i$ or $g_a - y_i$ then $\{x_i + g, y_i + g\} = \{g_a, g_b\}$. Thus every 2-subset of G belongs to the set $\{\{x_i + g, y_i + g\}\}$ so each 2-subset must occur exactly once. The latinicity of the first row follows from the definition of a starter, and of the first column from the definition of an adder. □

Exercise 11. Show that there exists no Room square of order 4 or 6.

Exercise 12. Construct a Room square of order 10 from the starter $\{\{1, 2\}, \{3, 7\}, \{4, 6\}, \{5, 8\}\}$ and the adder $(1, 7, 2, 8)$.

Theorem 22. *If there exists a strong starter in an abelian group of order $2n-1$ then there exists a Room square of order $2n$.*

Proof. An adder A is given by $A = (-x_1 - y_1, -x_2 - y_2, \dots, -x_{n-1} - y_{n-1})$. Indeed, writing $x_i + a_i = -y_i$, $y_i + a_i = -x_i$ shows that $\{x_i + a_i, y_i + a_i : i = 1, \dots, n-1\} = \{-x : x \in G \setminus 0\} = \{x : x \in G \setminus 0\}$ which means that A is an adder. □

A very general result is due to Mullin and Nemeth.

Theorem 23. *Let p be an odd prime such that $p^n = 2^k t + 1$ where $t > 1$ is odd. Then there exists a strong starter in GF(p^n).*

Theorem 24. *(The Existence Theorem for Room Squares.) A Room square of order n exists if and only if n is even, and $n \neq 4$ or 6.*

A generalization of a Room square is *Howell design.* A Howell design $H(s, 2n)$ on a set S, $|S| = 2n$, is an $s \times s$ array H such that

(i) every cell of H is either empty or contains a 2-subset of S,

(ii) each element of S is contained in exactly one cell of each row and each column of H, and

(iii) every 2-subset of S is contained in at most one cell of H.

A Howell design $H(2n-1, 2n)$ is the same as a Room square of order $2n$. The *underlying graph* of H is the s-regular graph with $2n$ vertices whose edges are the 2-subsets occurring in the nonempty cells of H. The underlying graph of a $H(2n-1, 2n)$ is the complete graph K_{2n}. A Howell design $H(s, 2n)$ whose underlying graphs is the complete bipartite graph $K_{s,s}$ is equivalent to a pair of MOLS(s). The existence theorem for Howell designs is as follows.

Theorem 25. *A Howell design $H(s, 2n)$ exists for all s, $n \leq s \leq 2n$, except when $(s, n) \in \{(2,4), (3,4), (5,6), (5,8)\}$.*

References

[1] T. Beth, D. Jungnickel, H. Lenz, *Design Theory, 2nd Edition, Vol.I, Vol.II*, Cambridge Univ. Press, 1999.

[2] C.J. Colbourn, J.H. Dinitz (Editors), *Handbook of Combinatorial Designs, 2nd Edition*, CRC Press, Boca Raton, 2007.

[3] C.J. Colbourn, A.Rosa, *Triple Systems*, Clarendon Press, Oxford, 1999.

[4] C.C. Lindner, C.A. Rodger, *Design Theory, 2nd Edition*, CRC Press, Boca Raton, 2009..

Further references

[AG] B. Alspach, H. Gavlas, *Cycle decompositions of K_n and $K_n - I$*, J. Combin. Theory (B) **81** (2001), 77–99.

[B] R.C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics **9** (1939), 353–399.

[CH] A.G. Chetwynd, A.J.W. Hilton, 1*-factorizing regular graphs of high degree - An improved bound*, Discrete Math. **75** (1989), 103–112.

[H] H. Hanani, *Balanced incomplete block designs and related designs*, Discrete Math. **11** (1995), 255–369.

[L] C.C. Lindner, *A partial Steiner triple system of order n can be embedded in a Steiner triple system of order* $6n + 3$, J. Combin. Theory (A) **18** (1975), 349–351.

[RR] C. Reid, A. Rosa, *Steiner systems $S(2, 4, v)$ - a survey*, Electron. J. Combin. **17** (2010), No.DS18.

[Saj] M. Šajna, *Cycle decompositions III: complete graphs and fixed length cycles*, J. Combin. Designs **10** (2002), 27–78.

[Sk] T. Skolem, *On certain distributions of integers in pairs with given differences*, Math. Scand. **5** (1957), 57–68.

[Sk1] T. Skolem, *Some remarks on the triple systems of Steiner*, Math. Scand. **6** (1958), 273–280.

[SL] G. Stern, H. Lenz, *Steiner triple systems with given subspaces; another proof of the Doyen-Wilson theorem*, Bull. Un. Mat. Ital. A **(5) 17** (1980), 109–114.

[W] R.M. Wilson, *An existence theory for pairwise balanced designs III: A proof of the existence conjectures*, J. Combin. Theory (A) **18** (1975), 71–79.